Security Review Report

Analysis of Threats and Mitigation Measures Based on Blockchain Connection Patterns

2024
The Digital Currency Forum Wallet Security Subcommittee

Contents

CONTENTS

Introduction

01

1.1 Purpose of Wallet Security Subcommittee and Placement of this Report

The Wallet Security Subcommittee has been studying the basic security requirements for systems utilizing the DCJPY Network to assist in the consideration of security measures by a wide variety of companies participating in the network, especially in the Business Zone.

This document is a reorganization of the “Security review report [key management]” and the “Security review report [distributed ledger],” which were written based on activities conducted from December 2020 to March 2024. The contents of this document are expected to be useful for understanding the characteristics of the distributed ledgers that comprise the DCJPY Network and to serve as a guide for considering more detailed security requirements in the future. The DCJPY network, which is the subject of this study, is based on specifications designed and implemented for PoC.

This document has been translated from the Japanese original issued in October 2024.

1.2 Background

The DCJPY Network is maintained through the participation and cooperation of not only the financial industry, including commercial banks, but also a wide variety of companies and organizations. To maintain the platform while multiple companies and organizations work together, it is essential to uphold a certain level of security for the systems managed by each company and organization and to improve the security of the entire platform.

There are currently a number of distributed ledger system constructions under consideration for use in a variety of fields, and the subcommittees of the Digital Currency Forum are also studying use cases and conducting demonstration experiments for linking the “distributed ledger system managed outside the DCJPY Network” and the “DCJPY Network,” as defined in Figure 1.2.

Some organizations participating in the DCJPY Network are required to comply with high security standards based on laws, regulations, and industry guidelines, whereas others are considering building new systems to enter the digital currency business. Although there are various differences in the ways of thinking about security measures, all organizations need to consider security measures based on an understanding of the unique characteristics of the DCJPY Network. Organizations in the DCJPY Business Zone will be required to take such measures.

Distributed ledger systems have an architecture of decentralized structures and authorities managed by multiple entities, some of which operate across industries and borders. A wide variety of services and software is expected to emerge sequentially because of the involvement of many stakeholders in distributed ledgers, including administrators, service providers, software developers, and development environment providers. Consequently, distributed ledger ecosystems have the potential to expand. However, the architecture of distributed ledger technology, such as decentralized structures and authorities, differs from that of traditional centralized systems, and systems that adopt distributed ledger technology must be constructed while considering these characteristics.

From a security perspective, it is necessary to consider the possibility that a problem in a particular system connected to a distributed ledger system could affect the distributed ledger system, or that a problem occurring in a distributed ledger system could affect other systems. However, distributed ledger technology involves a variety of functions and technical elements, and because they are intricately interrelated, security threat factors vary and are difficult to understand. It is necessary to analyze the elements involved in distributed ledger technology and consider the potential threats to these elements, and mitigate the risks posed by those threats.

Therefore, we decided to study and analyze security issues and mitigation measures in the Business Zone system from the perspective of building and operating a system that connects to the distributed ledger systems outside the DCJPY Network as defined in Figure 1.2.

1.3 Target Readership

The intended audience for this document includes:

1. **The Digital Currency Forum participants, who want to better understand the security issues involved in connecting the DCJPY Network to the distributed ledger systems that are operated by external organizations or communities.**

2. **System developers (especially distributed ledger engineers) and all those involved in security who are considering building systems for the Business Zone using the DCJPY Network.**

3. **Managers who consider future security policies for distributed ledger systems connected to the DCJPY Network.**

1.4 Prerequisite

This section is a summary of the prerequisites for this document.

1.4.1 About DCJPY Network

1.4.1.1 Layered Structure

The DCJPY Network is envisioned to have two areas, the “Financial Zone” and the “Business Zone,” for minting, transferring, and burning digital currency, which is called DCJPY, and a mechanism to connect the two areas (Figure 1.1).

The Financial Zone provides common functions in the DCJPY Network such as maintaining a ledger to record digital currency balances and providing a mechanism to connect to each bank's digital currency mining system.

The Business Zone is an area where application programs can be developed and deployed according to the specific requirements of the use case. The application programs can be designed, configured and operated independently of each other within the Business Zone. For more information on the overall structure, functions, and features of the DCJPY Network, please refer to the DCJPY White Paper.

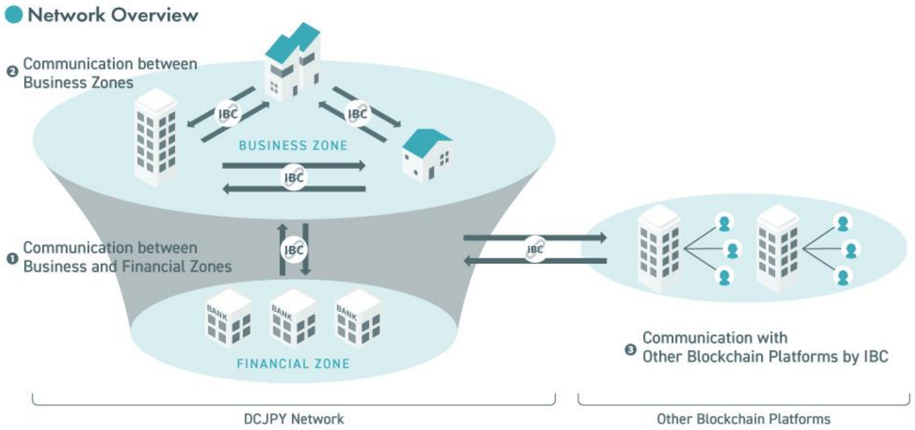
Network Overview
❷ Communication between Business Zones
IBC
IBC
BUSINESS ZONE
IBC
❶ Communication between Business and Financial Zones
IBC
IBC
BANK
BANK
BANK
FINANCIAL ZONE
❸ Communication with Other Blockchain Platforms by IBC
DCJPY Network
Other Blockchain Platforms

Figure 1.1 Overall View of the DCJPY Network

●出典　DCJPY White Paper https://amicsign.com/index.html

1.4.1.2 Network System

The distributed ledger used in the DCJPY Network is currently assumed to be “Hyperledger Besu” (named Besu with the launch of LF Decentralized Trust in September 2024), which is a consortium-type blockchain with a limited number of participating nodes, unlike so-called public blockchains (permissionless blockchains) such as Bitcoin and Ethereum.

In addition, a closed private network is established rather than an open public network based on the Internet. Therefore, it is expected that different security requirements will be required compared to public blockchains.

1.4.1.3 Components

The DCJPY Network comprises a set of software packages, called core packages, and signature keys for digital signatures to use them. The core packages are executed in the environment of each company or organization participating in the DCJPY Network, and the overall functionality of the DCJPY Network is achieved through the cooperative operation of these functions.

Owing to the decentralized structure of the DCJPY Network, it is unlikely that a partial failure will result in immediate shutdown of the entire platform. However, if an individual company or organization experiences a security problem, it could cause damage to the information assets and users under its control and, in some cases, could lead to a loss of trust in the DCJPY Network itself. To realize a trusted and secure digital currency platform, each company or organization must appropriately manage the platform’s software suite and various signature keys.

1.5 Scope of Analysis

This document identifies system security issues in the Business Zone that connect to and use distributed ledger systems of external organizations or communities. It also examines risk mitigation measures for these systems. Figure 1.2 shows the relationship between the distributed ledger systems of external organizations or communities and those of the Business Zone, highlighting the focus of this document's discussion.

- Service providers in the Business Zone are connected to the DCJPY Network for DCJPY remittances.
- In Figure 1.2, the applications in the Business Zone connected to the DCJPY Network are called the "DCJPY Business Applications," and the processing system connected to the DCJPY Network is called the "Business Zone Connection System."
- The Financial Zone of the DCJPY Network handles processes related to the mining, management, and burning of the DCJPY.
- Please note that this document will not provide a detailed overview of the Business Zone Connection System, the Financial Zone Connection System, and the DCJPY Network, which encompasses a private permissive distributed ledger system (blockchain) for processing the DCJPY.

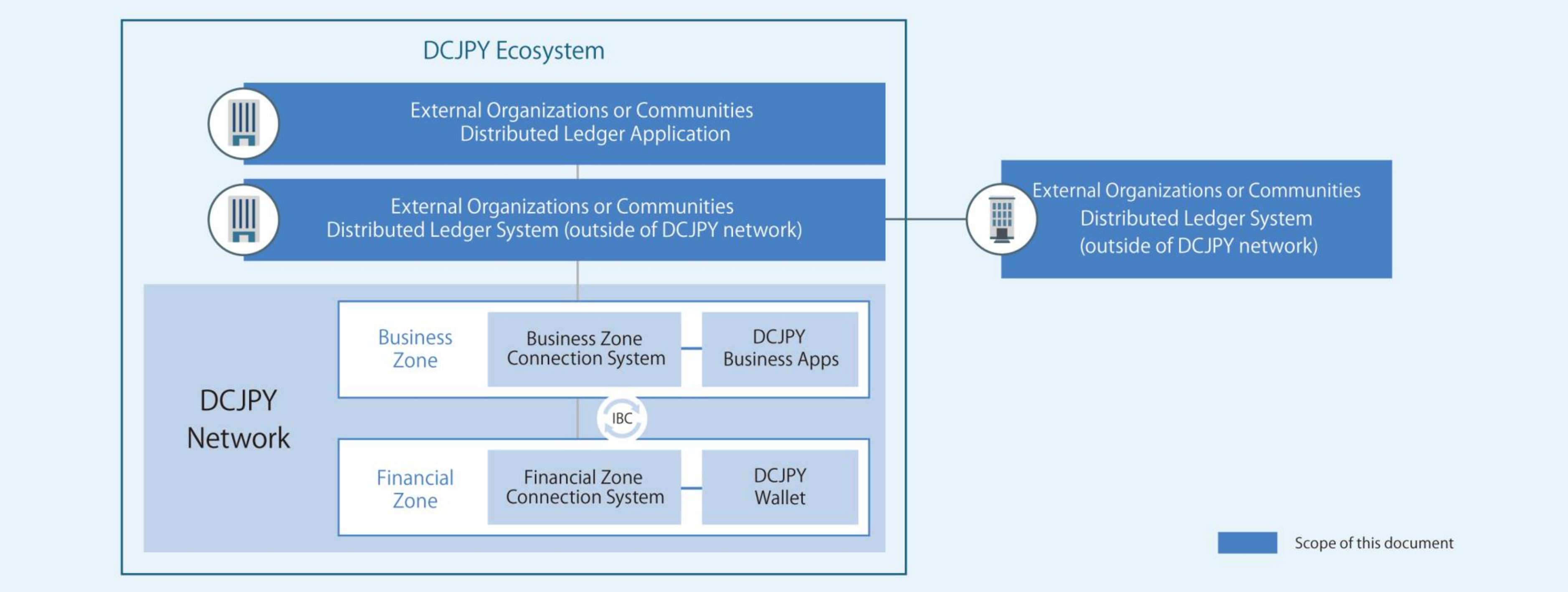
DCJPY Ecosystem
External Organizations or Communities Distributed Ledger Application
External Organizations or Communities Distributed Ledger System (outside of DCJPY network)
External Organizations or Communities Distributed Ledger System (outside of DCJPY network)
DCJPY Network
Business Zone
Business Zone Connection System
DCJPY Business Apps
IBC
Financial Zone
Financial Zone Connection System
DCJPY Wallet
Scope of this document

Figure 1.2: Scope of the Systems Covered in this Document

1.5 Scope of Analysis

This document assumes that the Business Zone system will be connected to a distributed ledger system by another external organization or community distinct from DCJPY's processing system. Such a system form may be configured when an external distributed ledger system is planned to manage digital assets independent of DCJPY management, or when the system is linked to a distributed ledger system already in operation prior to the introduction of DCJPY. It is also possible that the vendors providing the service in the Business Zone are (or are part of) the administrators of such a distributed ledger system.

This document addresses the security implications of external distributed ledger systems for services and systems established in the business zone. The following security issues have been discussed, although it should be noted that this list is not exhaustive.

- **General security issues that may potentially exist in distributed ledger platforms**
- **General security issues that may potentially exist in distributed ledger systems**
- **General security issues when managing distributed ledger nodes**
- **General security issues related to smart contracts**
- **Issues related to the configuration and operation of the Business Zone system**

The following are out of this scope.

- Legal conformities of businesses and systems in Business Zone
- Economic risks associated with digital assets
- Safeguards in the use of the DCJPY Network
- Details of general security measures in the Business Zone system
- Specific designs of the Business Zone system functions, protocols, processes, etc.

1.6 Glossary

Here is a list of terms that will help you as you read through this document.

■ Table: Glossary List

Term	Definition
IBC	One of the mechanisms for exchanging data and value between blockchains.
DCJPY	One of the digital currencies minted by banks.
DCJPY Wallet	Personalized screens connected to the BPM system managed by each bank and operated by the individual user, who is an account holder. (Also known as : Financial Zone Application)
DCJPY Business Apps	An application that allows the users to operate Business Zone. (Also known as: Business Application)
DCJPY Business Wallet	Corporate screens connected to the BPM system managed by each bank and operated by the legal entity user, who is an account holder.
DCJPY Network	A system that connects two blockchains with interoperability: the Financial Zone, which handles the money flow through DCJPY, and the Business Zone, which handles the commercial flow.
Business Zone	Blockchain handles the commercial flow on the DCJPY platform.
Financial Zone	Blockchain handles the money flow through DCJPY on the DCJPY platform.
Distributed Ledger Platform	Software that provides the basic functions of a distributed ledger, such as processing data, storing a ledger and communicating nodes.
Distributed Ledger System	A system that actually implements a distributed ledger using a distributed ledger platform. It consists of a network of nodes. This document uses the term "distributed ledger system" to refer to the distributed ledger system of the external organization or community described in the section titled "Scope of Analysis ."
Distributed ledger node or DLT node	A device or process that connects to a distributed ledger network and stores a copy of the ledger. While a function of transaction creation is sometimes differentiated as a DLT client, this function of transaction creation is treated here as one of the functions of a distributed ledger node.

Anticipated Connection Patterns with Distributed Ledger

02

CONTENTS

2.1 Introduction

A wide variety of use cases for ledger systems connected to the DCJPY Network is possible, and the internal configuration of the system in the Business Zone may be completely different for each use case. Various use cases are currently under discussion in the subcommittees of the Digital Currency Forum, with the expectation that a range of system configurations will emerge in the future. To identify common security issues and facilitate a more in-depth discussion on measures to address them, it would be beneficial to have more concrete systems in place. For this reason, we provided an example of a system configuration that serves as a basis for consideration.

This section provides an overview of the system configuration. Please note that this system is only an example, as mentioned above, and the actual system configurations may differ depending on its use. However, even in cases with different system configurations, the differences from the system configuration shown in this section can be identified, and the differences in security considerations caused by these differences can be discussed. We discuss the three models that are most likely to be used in actual operations.

2.2 Classification of Distributed Ledger System

This section classifies common forms of distributed ledger systems based on ISO 23257:2022, "Blockchain and distributed ledger technologies - Reference architecture." The distinction between public and private, and between permissionless and permissioned, defines the classification of ledger systems.

2.2.1 Public and Private

A public distributed ledger is a model that allows all nodes connected to the distributed ledger network to read ledger data, which are the transaction data listed in the ledger, as shown in Figure 2.1.

In contrast, a private distributed ledger allows only a specific group of nodes to read ledger data (Figure 2.2).

One approach for implementing a private distributed ledger is to place a public distributed ledger platform within a closed communication network, limiting access to specific nodes. Another approach is to control node access using a permissioned distributed ledger, as discussed subsequently.

Several models can be considered for writing the ledger data. One such model is open to all nodes, as exemplified by Bitcoin's Proof of Work. Another model allows only certain nodes to generate ledger data. Both models can be classified as public types. For further details, please refer to the Public Permission paragraph.

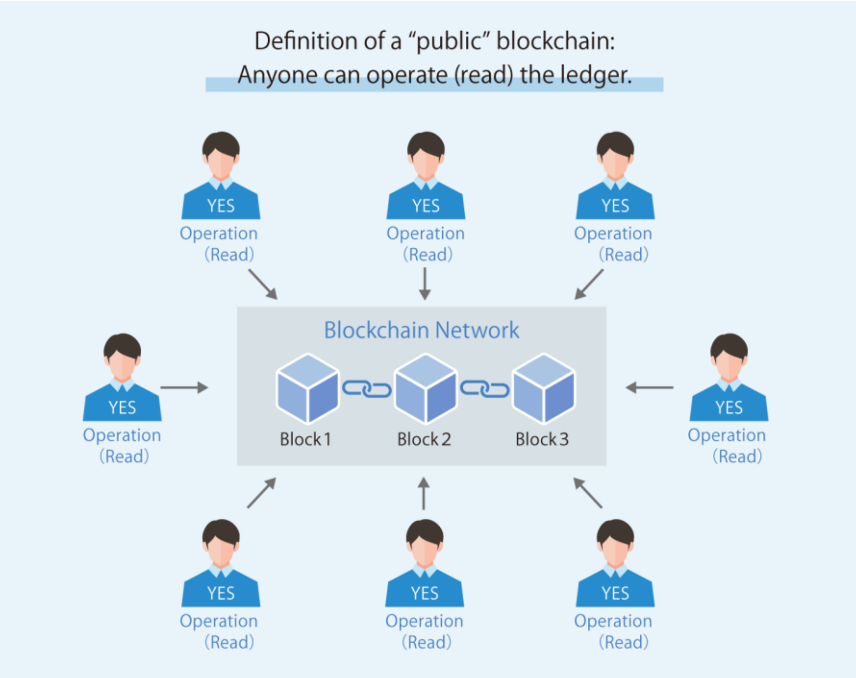
Definition of a "public" blockchain:
Anyone can operate (read) the ledger.
YES
Operation (Read)
Blockchain Network
Block 1
Block 2
Block 3

Figure 2.1 Concept of Public Distributed Ledger

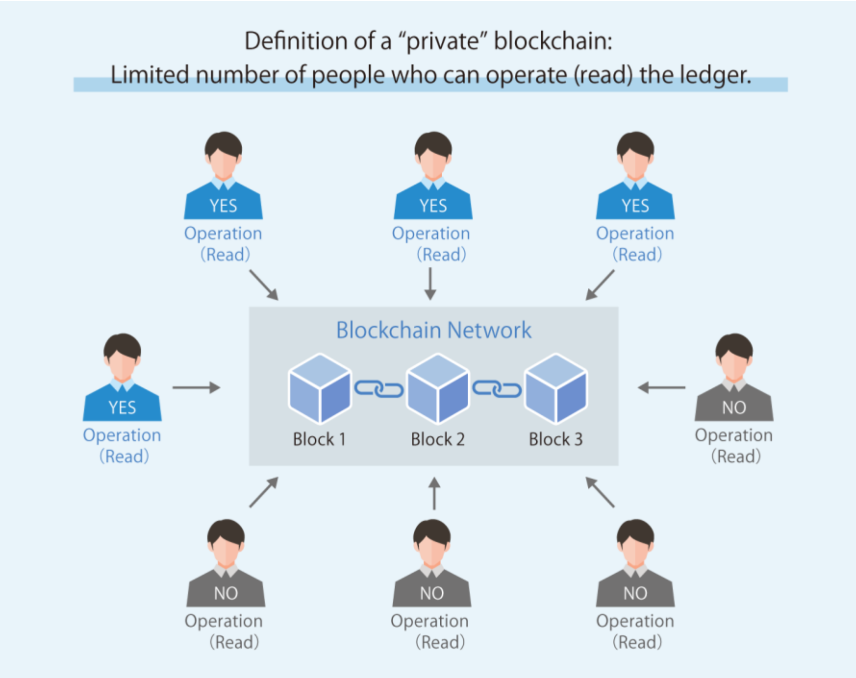
Definition of a "private" blockchain:
Limited number of people who can operate (read) the ledger.
YES
NO
Operation (Read)
Blockchain Network
Block 1
Block 2
Block 3

Figure 2.2 Concept of Private Distributed Ledger

2.2 Classification of Distributed Ledger System

2.2.2 Permissionless and Permissioned

The distinction between permissionless and permissioned relates to the necessity of permissions to connect to a distributed ledger system. In the case of permissionless distributed ledger platforms, there is no access control or permission capability for node connections (Figure 2.3).

In contrast, the permissioned type is a mechanism with procedures related to connection permissions and access control functions (Figure 2.4).

For example, distributed-ledger platforms that can be designed as the permissioned type include Hyperledger Fabric, Hyperledger Besu, and R3 Corda.

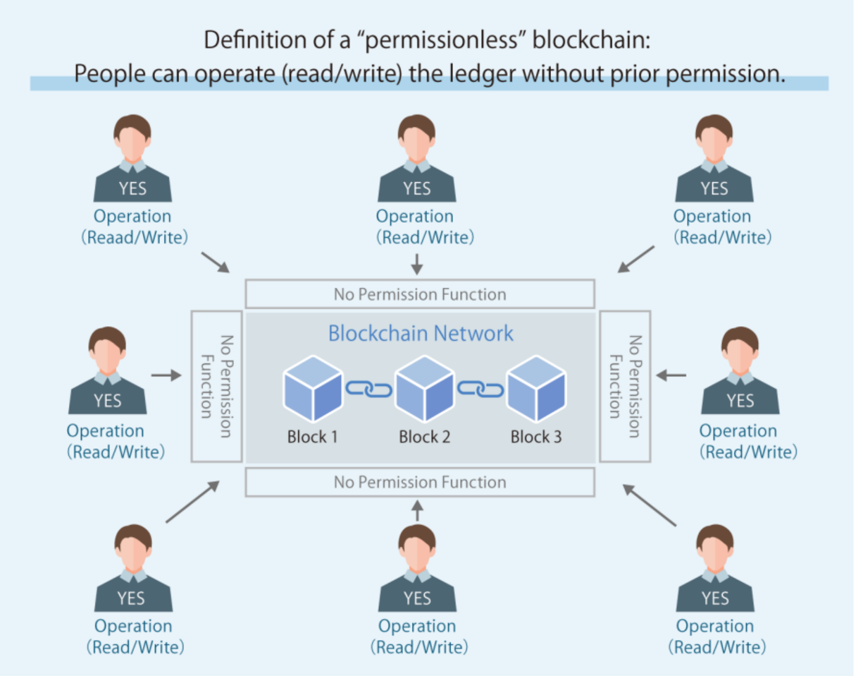
Definition of a "permissionless" blockchain:
People can operate (read/write) the ledger without prior permission.

Figure 2.3 Concept of Permissionless Distributed Ledger

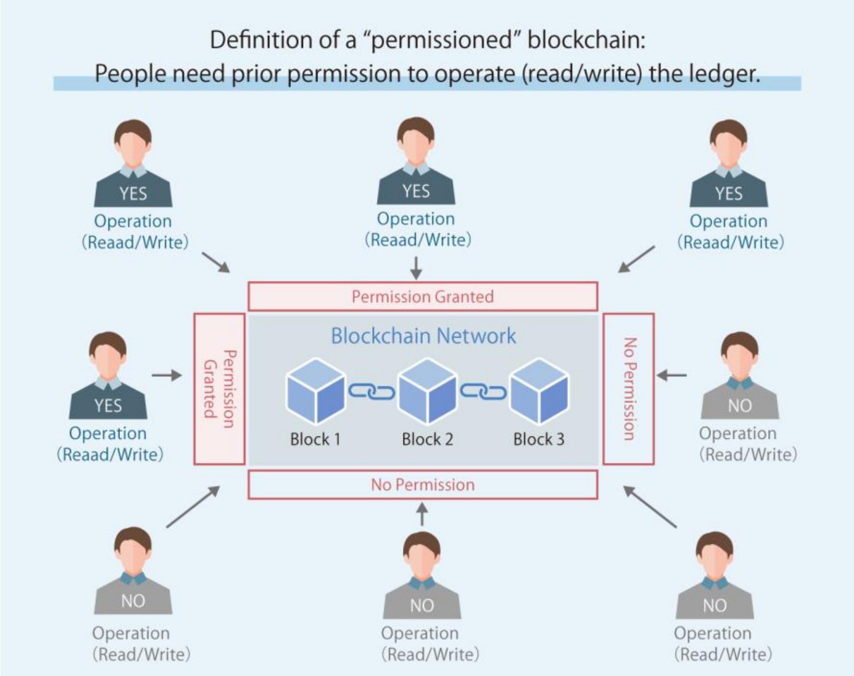
Definition of a "permissioned" blockchain:
People need prior permission to operate (read/write) the ledger.

Figure 2.4 Concept of Permissioned Distributed Ledger

2.2 Classification of Distributed Ledger System

The distinction between public and private and that between permissionless and permissioned are independent, and there can be forms that combine both distinctions, depending on the platform architecture and deployment methods.

- **Public Permissionless**
  This model is designed to enable users to read and write to ledger data. There are no pre-authorization or access restrictions for the connections. For example, the Bitcoin and Ethereum networks, which are used in various locations around the globe, are included in this category.

- **Public Permissioned**
  While any user can view the ledger data, writing to ledger data is limited to specific nodes that have been authorized in advance. For example, when managing data related to food traceability in a ledger, all nodes connected by consumers can view the information on food distribution channels described in the ledger data, whereas writing to the ledger data is limited to those involved in food distribution.

- **Private Permissionless**
  In a distributed ledger platform, this model does not have permission or access control mechanisms for the connected nodes. However, only certain nodes can operate the platform with restrictions such as the environment in which the platform is operated. For example, the Bitcoin or Ethereum platform software can be deployed and operated on a closed communication network, allowing the construction of a unique distributed ledger network to which only a limited number of nodes can connect.

- **Private Permissioned**
  This model builds a distributed ledger network that can be operated only by specific nodes using a distributed ledger platform with permission mechanisms for ledger data manipulation.

For example, this is the case with a distributed ledger network using Hyperledger Fabric, Besu, for use within an industry. The distributed ledger, which serves as the basis for the Financial Zone and Business Zone of the digital currency platform is also structured in this form.

This document focuses on two representative examples of external distributed ledger systems handled by the Business Zone systems connected to the DCJPY Network: the "public permissionless" case and the "private permissioned" case.

The former case is intended to be connected to networks of cryptographic and digital assets that already have many users worldwide, whereas the latter case is intended to establish a distributed ledger system among companies in the Business Zone that is used for a specific industry and linked to the DCJPY.

It is anticipated that the remaining permissioned public and private cases will present issues similar to those discussed in this document. Consequently, these are likely to be examined based on the discussion in this document.

2.3 Example of System Model for Business Zone using Distributed Ledger System

This document discusses the following three types of Business Zone systems that use public permissionless and private permissioned distributed ledger systems. A fictitious organization, “XYZ,” is assumed as a company in the Business Zone and the system managed by XYZ is considered.

- **Anticipated System Model 1**
  (Public Permissionless with Custodial Wallet Type)
  XYZ uses a public permissionless distributed ledger system to conduct transactions of digital assets and DCJPY. XYZ conducts transactions involving end users’ digital assets on behalf of end users.

- **Anticipated System Model 2**
  (Public permissionless with Non-Custodial Wallet Type)
  In another case, XYZ uses a public permissionless distributed ledger system to conduct transactions of digital assets and DCJPY. End users’ digital assets are managed via their own wallets.

- **Anticipated System Model 3**
  (Private Permissioned)
  XYZ conducts digital asset transactions via a private permissioned distributed ledger system jointly managed by XYZ within the industry. XYZ provides end users with interfaces and other services related to digital assets.

The following assumptions apply in these cases.

(Preconditions for Anticipated Use)
<u>About XYZ Services</u>

- XYZ provides an online platform to buy and sell digital assets. Digital assets are traded between the end users of a service.
- XYZ is positioned as a company in the Business Zone.
- XYZ uses XYZ Coins, the Business Zone currency issued under DCJPY.
- Digital assets can be bought and sold in XYZ Coins. End users create accounts for the service, which is managed by XYZ when using this service. When logging into this service, they use the account for their ID.
- The online service is provided by the Business Zone system, managed by XYZ.
- The Business Zone system is connected to the DCJPY Network to provide instructions for the transfer of XYZ Coins. The Business Zone system is responsible for managing signature keys that are used to connect to the DCJPY netwokr.
- The Business Zone system is connected to a distributed ledger system that manages the digital assets. The specific type of connection varied depending on the anticipated system model.
- The execution of smart contracts or the exchange of digital assets in a distributed ledger system may require the cryptographic assets of that distributed ledger system, e.g. ETH. of that distributed ledger system. However, the Business Zone system is assumed to have the necessary cryptographic assets, etc. in advance. In This case, XYZ is responsible for the management of cryptographic assets. The Business Zone system manages the signature keys required to transfer cryptographic assets. Please note that functions related to the exchange of digital assets and cryptographic assets, as well as the exchange between XYZ Coins and cryptographic assets, fall outside the scope of this document.

2.4 Anticipated System Model 1 (Public Permissionless with Custodial Wallet Type)

In Anticipated System Model 1, the system in the XYZ Business Zone is connected to a public permissionless distributed ledger system that manages digital assets. The Business Zone system then handles operations such as minting and transferring digital assets to a distributed ledger system. Therefore, XYZ is responsible for managing the signature keys to create transactions that transfer digital assets.

Ethereum is used as an example of a public permissionless distributed ledger system to illustrate the concept more clearly. However, the following discussion is not limited to Ethereum but is also applicable to other public permissionless distributed ledger systems.

The Business Zone system should be ready for use at the beginning of the service period, assuming that the following conditions are satisfied:

Conditions

- Provide end users with a digital authentication solution for logging in and executing digital asset transactions as a service for XYZ. Alternatively, authentication can be provided by another (e.g., a device authenticator).
- Once the end-user registration process is complete, the end user is granted access to XYZ's services.
- The Business Zone system provides end users with a marketplace user interface for digital assets, e.g. NFT.
- The provision method may be provided in the form of either a web or smartphone application. Figure 2.5 shows an example smartphone application.

Preliminary preparation

- Creating connection information, such as signature keys, blockchain addresses, and user accounts, to connect the distributed ledger system.
- Acquisition of cryptographic assets necessary for service implementation.
- Configuring the DCJPY Network includes the generation and registration of signature keys.
- Creating a DCJPY account and setting up a DCJPY wallet, which is provided by the Financial Zone.
- Account registration procedures required for XYZ's service, including registration of a DCJPY account and integration of DCJPY wallets.

2.4 Anticipated System Model 1 (Public Permissionless with Custodial Wallet Type)

Figure 2.5 presents an illustration of the Anticipated System Model 1. This figure uses NFTs as an example of a digital asset for transactions.

The Business Zone system accesses data from the distributed ledger system to generate a list of digital assets (NFTs) that can be traded. For instance, in the case of an NFT pertaining to a digital image, the system may retrieve and display the digital image to which it refers.

The connection to the distributed ledger system is established through distributed ledger nodes within the Business Zone system. Based on data acquired from the distributed ledger system, the business logic server identifies the end-user information (account managed by XYZ) that holds the right to digital assets and the price of digital assets. Based on the results, the NFT marketplace function of the Business Zone system is leveraged to create displays for users, as needed.

Diagram of a full agency model of a service vendor developing a blockchain game

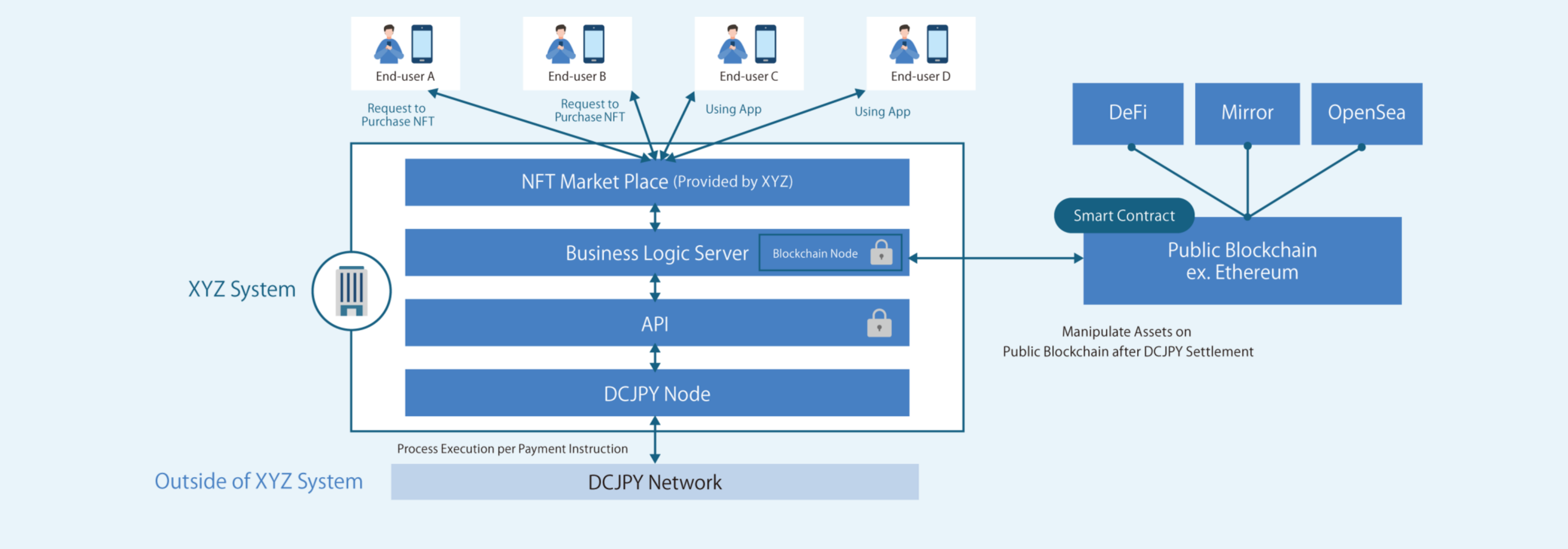

Figure 2.5 Anticipated System Model 1

2.4 Anticipated System Model 1 (Public Permissionless with Custodial Wallet Type)

Figure 2.6 illustrates the process of purchasing an NFT by an end user. This diagram presents a simplified overview of the process by which an end user purchases a new NFT issued by XYZ. The number of steps may vary depending on the system design.

- The end user issues instructions for purchasing digital assets through the NFT Marketplace user interface. These requests are made via the NFT Marketplace user interface, provided by the Business Zone system, on the end user's smartphone and other devices. The requests are then processed using the business logic server.

- When XYZ coins require transfers, a request for a money transfer operation is issued to the end user through the NFT Marketplace. The end user then creates remittance instructions using the DCJPY wallet functionality. Remittance instructions are transmitted to the Financial Zone via the Business Zone system (not shown in Figure 2.6), where the remittance process is executed.

- To perform an operation on the distributed ledger system, such as instructing the issuance of a token for a digital asset or transferring a token to the user account, a transaction is created and sent to the distributed ledger system via distributed ledger node. At this point, a smart contract deployed in the distributed ledger system may also be executed. A smart contract may be developed by XYZ or, alternatively, it may utilize a third-party smart contract. The business logic server then interacts with the results of smart contract execution and performs the necessary processing.

- The business logic sever updates the transaction status of the digital assets based on the results of the XYZ Coin transfer process and the digital asset transfer process and returns the results to the end user.

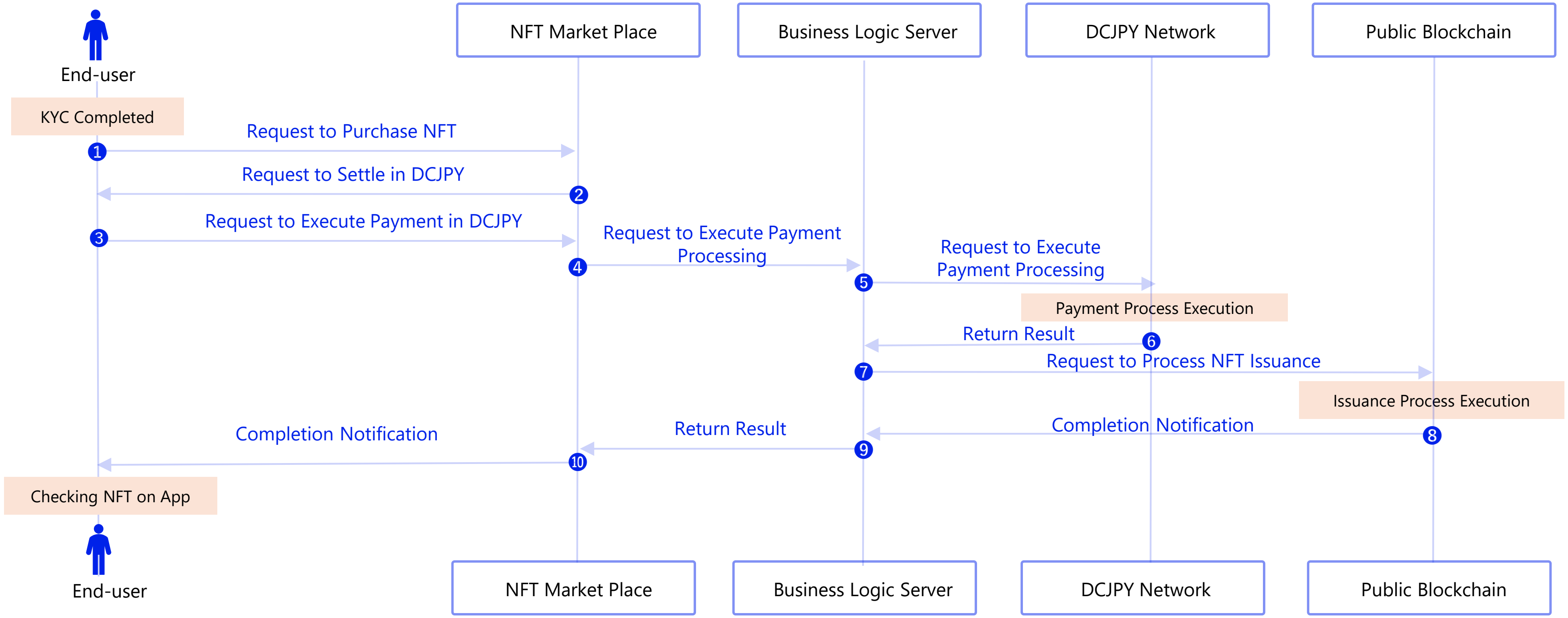
NFT Market Place
Business Logic Server
DCJPY Network
Public Blockchain
End-user
KYC Completed
1 Request to Purchase NFT
2 Request to Settle in DCJPY
3 Request to Execute Payment in DCJPY
4 Request to Execute Payment Processing
5 Request to Execute Payment Processing
Payment Process Execution
6 Return Result
7 Request to Process NFT Issuance
Issuance Process Execution
8 Completion Notification
9 Return Result
10 Completion Notification
Checking NFT on App
End-user
NFT Market Place
Business Logic Server
DCJPY Network
Public Blockchain

Figure2.6 Example Flow of Anticipated System Model 1

2.5 Anticipated System Model 2 (Public Permissionless with Non-Custodial Wallet Type)

Anticipated System Model 2 is a case in which end users assume responsibility for managing their own digital asset wallets, which in turn manage the signature keys for their digital assets. Digital assets are managed using a public, permissionless distributed ledger system. The system in the XYZ Business Zone does not manage the end user's digital asset signature keys; rather, it manages information about digital assets and the end user.

For simplicity, we use Ethereum as an example of a public permissionless distributed ledger system. The following discussion is not limited to Ethereum but is also applicable to other public permissionless distributed ledger systems.

At the beginning of the service period, the following conditions have been met:

Conditions

- Prior to utilizing the service, end users have already configured a digital asset wallet and are responsible for managing the signature key for the transfer of digital assets.
- The DCJPY account must be opened and the DCJPY wallet configured.
- The Financial Zone provides procedures for opening DCJPY accounts and wallets.
- To use XYZ's services, it is necessary to complete an account registration process. This includes registering digital asset wallets, DCJPY accounts, and DCJPY wallet linkages.
- The method of linking digital asset wallets to XYZ service accounts varies depending on the type of wallet, as digital asset wallets can take many forms and are selected by end users. This document does not present a specific linking method but outlines the general process to be followed.

Preliminary preparation

- Configuring the DCJPY Network includes the generation and registration of signature keys.
- Deploying smart contracts linked to the NFT marketplace on a distributed ledger system.

2.5 Anticipated System Model 2 (Public Permissionless with Non-Custodial Wallet Type)

Figure 2.7 presents an illustration of Anticipated System Model 2. This figure uses NFTs as an example of a digital asset for transactions.

XYZ provides end users with a means of authentication to log into its services and execute digital asset transactions. Alternatively, it may adopt a means of authentication provided by another entity such as another device authenticator, a digital asset wallet, or a feature provided by a DCJPY wallet.
Once the end-user registration process is complete, the end user is granted access to XYZ's services.
The Business Zone system provides end users with a user interface to the marketplace of digital assets, such as NFTs. The method of provision could take the form of a web or smartphone application. Figure 2.7 illustrates the smartphone interface.

The Business Zone system acquires data on digital assets from the distributed ledger system based on the data provided by the end user, e.g., remittance address and remittance amount, and displays a list of tradable digital assets (NFTs). The business logic server identifies the user’s rights to digital assets based on the user account information managed by XYZ and data acquired from the distribute ledger system. Using the results, the NFT marketplace function of the Business Zone system is leveraged to create displays for users as needed.

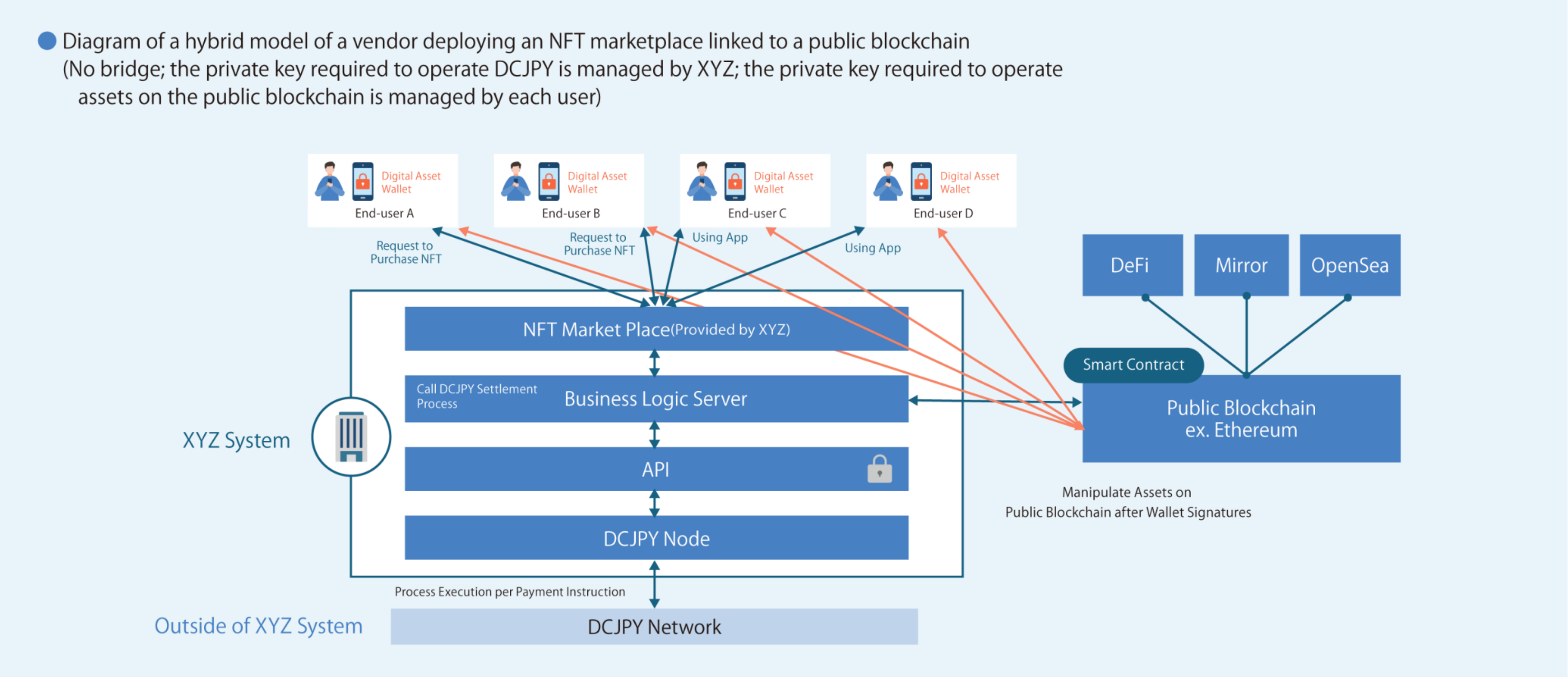
Diagram of a hybrid model of a vendor deploying an NFT marketplace linked to a public blockchain
(No bridge; the private key required to operate DCJPY is managed by XYZ; the private key required to operate assets on the public blockchain is managed by each user)
Digital Asset Wallet
End-user A
Digital Asset Wallet
End-user B
Digital Asset Wallet
End-user C
Digital Asset Wallet
End-user D
Request to Purchase NFT
Request to Purchase NFT
Using App
Using App
DeFi
Mirror
OpenSea
NFT Market Place(Provided by XYZ)
Smart Contract
Call DCJPY Settlement Process
Business Logic Server
Public Blockchain ex. Ethereum
XYZ System
API
Manipulate Assets on Public Blockchain after Wallet Signatures
DCJPY Node
Process Execution per Payment Instruction
Outside of XYZ System
DCJPY Network

Figure 2.7 Notional System Model 2

2.5 Anticipated System Model 2 (Public Permissionless with Non-Custodial Wallet Type)

Figure 2.8 illustrates the process of purchasing an NFT between end users. This process may vary depending on the design specifications.

- End user 1 purchases the digital asset held by end user 2. First, in advance of the transaction, end user 2 operates their own digital asset wallet and transfers the digital asset they want to sell to a smart contract in a distributed ledger system. This smart contract is linked to the NFT marketplace and can be operated using the business logic server.
- End user 1 issues instructions to purchase digital assets for end user 2 via the NFT Marketplace user interface. These requests are made via the end user's smartphone or other devices to the NFT Marketplace user interface provided by XYZ service.
- These requests made to the NFT marketplace are processed by the business logic server, which then requests the payment of XYZ coins for the digital asset from end user 1.
- End user 1 remits payment to end user 2 in XYZ coins via DCJPY wallets.
- After the NFT Marketplace receives confirmation of the payment, it instructs the smart contract to transfer the digital asset belonging to end user 2 to end user 1's distributed ledger address.
- The business logic server updates the transaction status of the digital asset based on the results of the XYZ Coin transfer process and the digital asset transfer process and returns the result to end users 1 and 2.

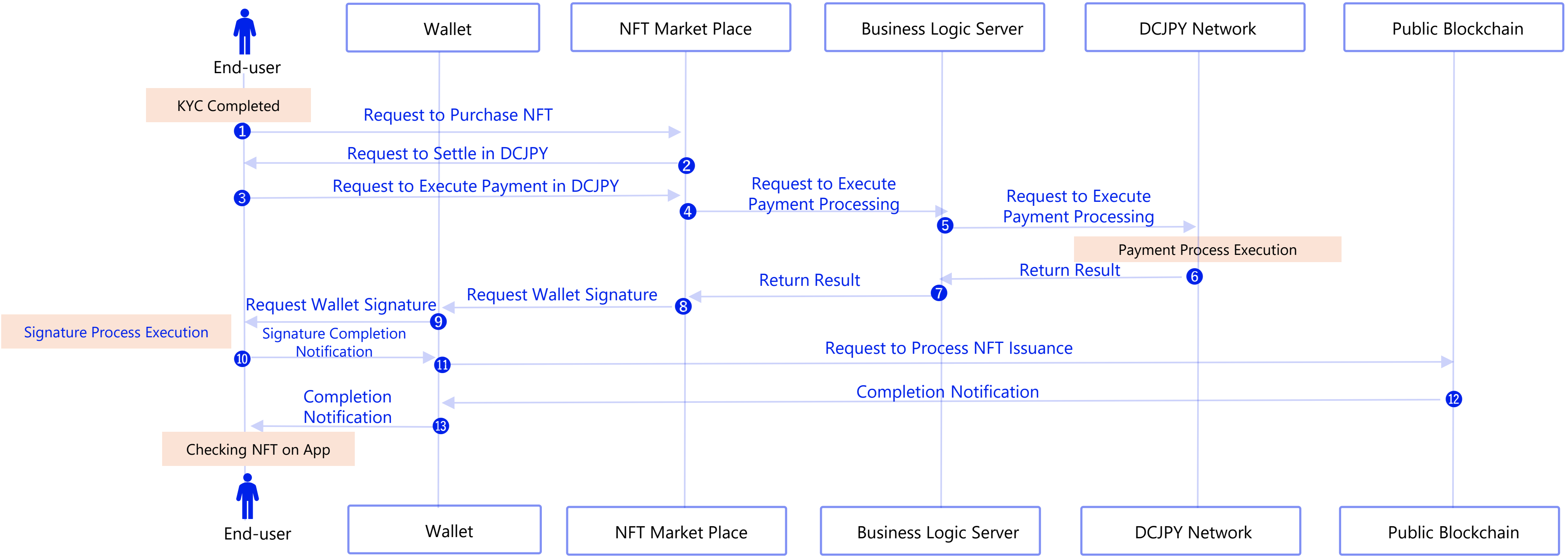
End-user
Wallet
NFT Market Place
Business Logic Server
DCJPY Network
Public Blockchain
KYC Completed
1 Request to Purchase NFT
2 Request to Settle in DCJPY
3 Request to Execute Payment in DCJPY
4 Request to Execute Payment Processing
5 Request to Execute Payment Processing
Payment Process Execution
6 Return Result
7 Return Result
8 Request Wallet Signature
Request Wallet Signature
Signature Process Execution
9 Signature Completion Notification
10
11 Request to Process NFT Issuance
12 Completion Notification
13 Completion Notification
Checking NFT on App
End-user
Wallet
NFT Market Place
Business Logic Server
DCJPY Network
Public Blockchain

Figure 2.8 Example Flow of Anticipated System Model 2

2.5 Anticipated System Model 2 (Public Permissionless with Non-Custodial Wallet Type)

For ease of illustration, XYZ Coins are paid directly from end user 1 to end user 2. To collect fees during the transaction, prevent erroneous transfers, and protect privacy among end users, it is possible to transfer the money to the DCJPY account of XYZ service, which may then transfer the money to end user 2.

When a digital currency transfer is required, a transfer request is issued to the end user through the NFT Marketplace. The end user creates a transfer instruction using the DCJPY wallet functionality. The remittance instruction is sent to the DCJPY Network via the Business Zone system and the remittance process is executed.

To operate the distributed ledger system, such as issuing instructions for NFTs or transferring NFTs between accounts, the business logic server creates transactions and sends them to the distributed ledger system via distributed ledger nodes. At this point, a smart contract deployed in the distributed ledger system may be executed. A smart contract may be developed by XYZ or, alternatively, it may utilize a third-party smart contract. The business logic server then interacts with the results of smart contract execution and performs the necessary processing.

The business logic server updates the transaction status of the digital asset based on the results of the XYZ Coin transfer process and the digital asset transfer process and returns the results to the end user.

2.6 Anticipated System Model 3 (Private Permissioned)

Anticipated System Model 3 is similar to Anticipated System Model 1, except that it connects to a private permissioned distributed ledger system.

The XYZ Business Zone system connects to the private permissioned distributed ledger system, which manages digital assets and performs operations such as transferring digital assets to the distributed ledger system.

In a private permissioned distributed ledger system, it is expected to demonstrate governance, including the following policies: Security management of the execution environment for each node connected to the system, Identity proofing, authentication, and authorization of administrators, Decision-making methods regarding policies and controls. By designing a distributed ledger system or smart contract based on appropriate governance, it may be possible to share distributed ledger data only among the group members involved and stop or revoke transactions, ledgers, or nodes connected to the system when problems arise through cooperation among administrators.

At the beginning of the service period, the following preparations have been completed:

Preliminary preparation

- Design and deployment of distributed ledger systems

  This distributed ledger system is operated by a consortium of companies with aligned objectives and policies. In addition to XYZ, Companies A, B, and C participate in the consortium and are responsible for managing their own distributed ledger nodes. It is not possible to connect nodes that are not a part of the consortium.

- Configuration required for the Business Zone system to connect to a distributed ledger system

  Examples include the creation and registration of authentication credentials (e.g., signing keys), blockchain addresses, and accounts for nodes.

- Configuration to use the DCJPY Network

  Examples include the generation and registration of signature keys for connections to the DCJPY Network.

2.6 Anticipated System Model 3 (Private Permissioned)

Figure 2.9 illustrates an example system for this model, while Figure 2.10 provides an example of the flow from NFT purchases to remittances. Hyperledger Fabric is used as the basis for discussions on private permissive distributed ledger systems. The following discussion is not limited to the Hyperledger Fabric but is also applicable to other privately permissioned distributed ledger systems.

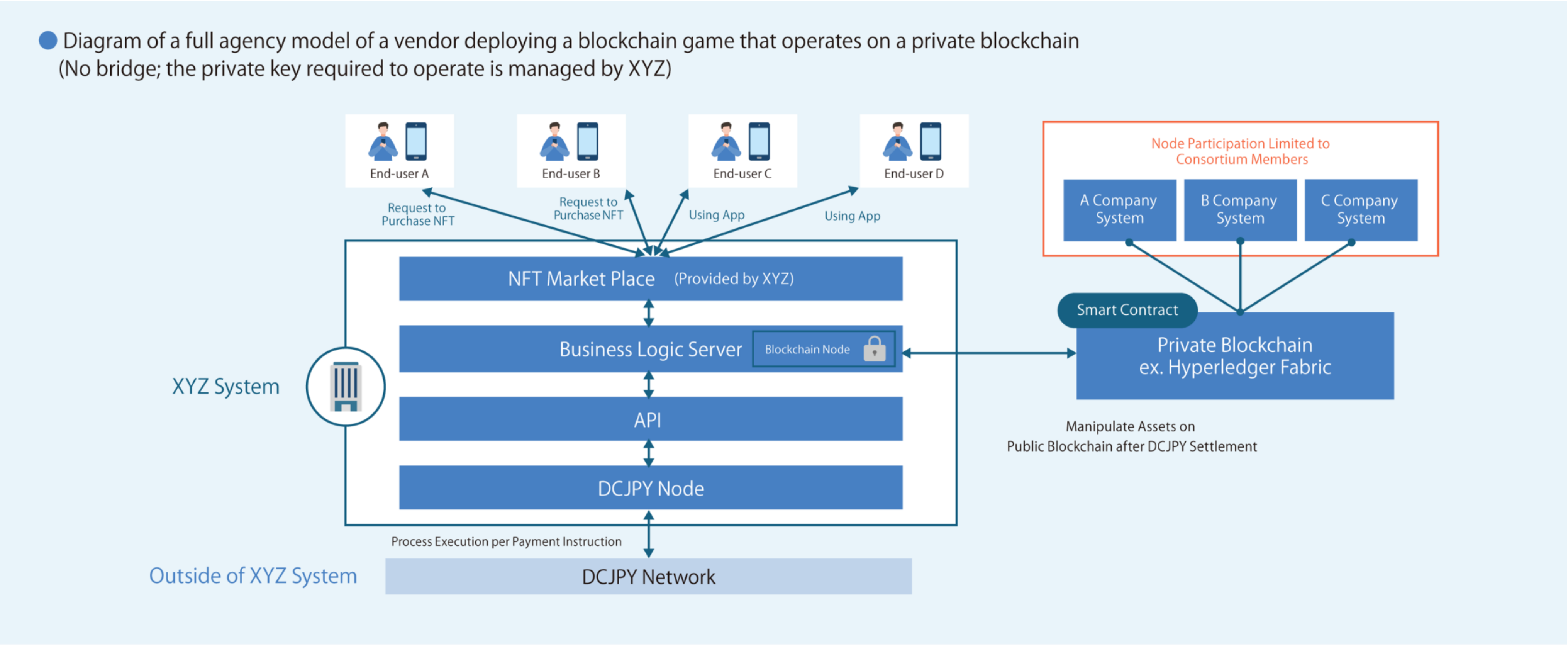
● Diagram of a full agency model of a vendor deploying a blockchain game that operates on a private blockchain
(No bridge; the private key required to operate is managed by XYZ)
End-user A
End-user B
End-user C
End-user D
Request to Purchase NFT
Request to Purchase NFT
Using App
Using App
Node Participation Limited to Consortium Members
A Company System
B Company System
C Company System
Smart Contract
Private Blockchain ex. Hyperledger Fabric
NFT Market Place (Provided by XYZ)
Business Logic Server
Blockchain Node
API
DCJPY Node
XYZ System
Manipulate Assets on Public Blockchain after DCJPY Settlement
Process Execution per Payment Instruction
Outside of XYZ System
DCJPY Network

Figure 2.9 Anticipated System Model 3

2.6 Anticipated System Model 3 (Private Permissioned)

The end-user registration process and the transaction of digital assets to the transfer of XYZ Coins are identical to those described in Anticipated System Model 1 (See Section 2.4).

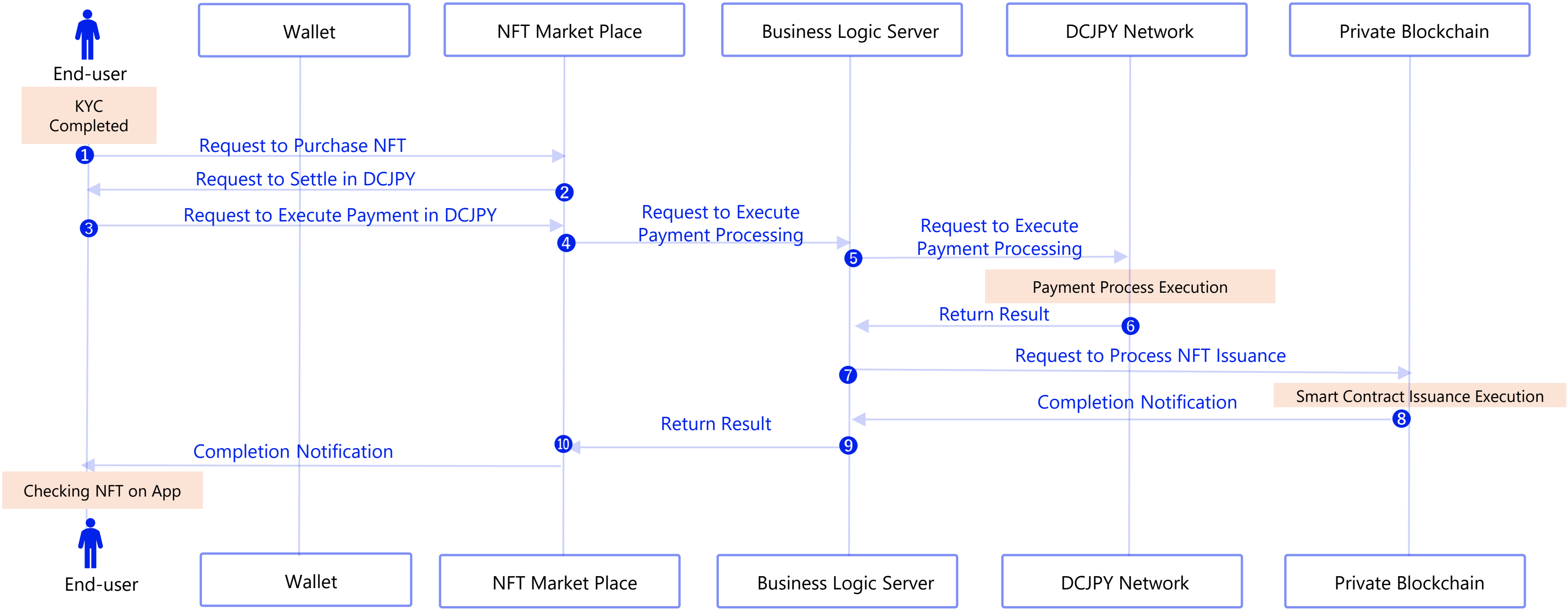
End-user
Wallet
NFT Market Place
Business Logic Server
DCJPY Network
Private Blockchain
KYC Completed
1 Request to Purchase NFT
2 Request to Settle in DCJPY
3 Request to Execute Payment in DCJPY
4 Request to Execute Payment Processing
5 Request to Execute Payment Processing
Payment Process Execution
6 Return Result
7 Request to Process NFT Issuance
Smart Contract Issuance Execution
8 Completion Notification
9 Return Result
10 Completion Notification
Checking NFT on App
End-user
Wallet
NFT Market Place
Business Logic Server
DCJPY Network
Private Blockchain

Figure 2.10 Example Flow of Anticipated System Model 3

03

Security Issues

CONTENTS

Chapter 3

Security Issues

3.1 Introduction

This chapter discusses the security-related risks and issues associated with each system model described in Chapter 2.

3.2 Security Issues Common to Anticipated System Model

3.2.1 Introduction

In this section, we discuss the general threats to the distributed ledger platform that provides basic distributed ledger functions, the distributed ledger system that is built and operated, and the nodes that make up the distributed ledger system. Following this, we examine the security issues for the Anticipated System Models 1 through 3.

3.2.2 Threats to Distributed Ledger Platform

3.2.2.1 Distributed Ledger Platform Considerations

The software that provides the essential functions of the distributed ledger system to which the Business Zone systems connect is referred to here as a "distributed ledger platform." Distributed ledger platforms are exemplified by Ethereum and Hyperledger Fabric.
A distributed ledger system is constructed when multiple nodes, each running distributed ledger platform software, operate cooperatively.

A distributed ledger system may be used in conjunction with a protocol called Layer 2, which extends the functionality and performance of the distributed ledger platform. Another auxiliary distributed ledger system, called a side chain, can also be used. Layer 2 may be applied between specific nodes of the distributed ledger system, and side chains may be operated by a different entity (group of nodes) than the underlying distributed ledger system. Layer 2 and side chain software can be developed by entities separate from the distributed ledger platform.

This section presents an in-depth examination of the underlying ledger platform. These considerations may also apply to Layer 2 and the side-chain software. While the focus of this section is on potential threats to the distributed ledger platform, it is important to note that not all threats may immediately compromise the actual distributed ledger system. The probability of a threat to a distributed ledger platform manifesting in an actual distributed ledger system is contingent on the percentage of nodes affected by the threat, among other factors. The potential threats to ledger systems are discussed in Subsection 3.2.3.

The underlying distributed ledger platform may typically include the following features and elements:

- Consensus mechanism
- Ledger management
- Transaction generation and validation
- Generate, deploy, and execute smart contracts
- Communication between nodes
- Authentication and authorization of nodes
- Cryptographic algorithm

There are two main categories of threats to distributed ledger platforms: design- and specification-based threats, and implementation-based threats. Design- and specification-based threats affect the entire implementation, whereas vulnerabilities in the implementation method affect the specific implementation to which the method is applied.

3.2.2.2 Consensus Mechanism

In distributed-ledger technology, several processes related to ledger generation, such as verifying transactions generated by different nodes, determining which transactions should be stored in the ledger, and storing transactions in the ledger, must be coordinated among multiple nodes. The mechanism for coordinating nodes to maintain ledger integrity is collectively referred to as the consensus mechanism.

Several consensus mechanism methods have been proposed that differ for each distributed ledger platform. Examples of consensus mechanism classifications are as follows (see ISO 23257).

- **Round-robin type**
  Multiple management nodes are set up and they generate ledgers on a rotating basis.

- **Practical byzantine fault tolerance type** [1]
  Integrity is maintained by multiple management nodes that validate each other's ledger-generation messages. In a Byzantine fault-tolerance mechanism, even in the event of a malware infection or other issues that result in incorrect messages being sent by some nodes, the number of nodes that can still share correct messages remains greater than the number of nodes that send incorrect messages.

- **Nakamoto consensus type**
  This mechanism encourages each node to participate voluntarily in the generation and coordination of the ledger by rewarding cryptographic assets without regulating a specific managing node. Typical examples are Bitcoin's Proof of Work and Ethereum's Proof of Stake.

In some cases, methods that are not Byzantine fault-tolerant, but only fault (outage) tolerant to node outages, may be used.

The consensus mechanism plays an important role in distributed-ledger technology for generating and sharing ledgers. Serious flaws in the design, specification, or implementation of the consensus mechanism can lead to threats such as unauthorized rewriting of ledger data, unauthorized replication, halted or delayed execution of transactions/smart contracts due to outages or delays in ledger generation, and control of nodes that are responsible for ledger generation.

The feasibility of the threat and the degree of impact if it occurs depend on the types of operations of the distributed ledger systems (classified in Section 2.2), the size of the network of nodes, and other factors. Although this depends on the nature of the vulnerability, in general, the larger the size of the nodes involved in the ledger generation, the less likely it is that a particular attacker will be able to realize fraud. Simultaneously, the larger the network size, the greater the impact of fixing software vulnerabilities and fraudulent ledgers.

It is important to evaluate the security of a distributed ledger platform by considering the characteristics of the consensus mechanism employed by the platform and the trust structure that guarantees the authenticity of the ledger, including the existence of the nodes involved in its creation and verification. Even if there are no unintentional flaws in the consensus mechanism, there is a risk that certain parties may take control of the ledger by exploiting its specification features. This is discussed in Subsection 3.2.3.5.

[1] For instance, if the number of unauthorized nodes is less than one-third of the total, the system will operate correctly.

3.2.2.3 Ledger Management

The ledger data generated by the consensus mechanism are replicated and managed at each node. A node that stores all ledger data is called a full node. Depending on how the ledger is replicated, the ledger held by one node may not match that held by another node at any given time. Temporary ledger data rewinding (reorg) can occur in a mechanism without the ledger data finality. Inconsistencies in the ledger data at each node or failures in the ledger data management mechanism may result in an inability to properly verify or confirm transactions (e.g., balance checks) that reference the ledger at that node. If there are problems with the specifications or implementations of the distributed ledger platform, and the impact is on a large scale, it may result in transfers, halts, or delays in ledger data and transactions throughout the distributed ledger system.

3.2.2.4 Transaction Generation and Validation

Failures in the transaction-generation function can result in a halt or delay in transaction processing. In addition, a serious vulnerability in the generation function poses a significant threat if it leads to the unauthorized generation of transactions by an attacker (unauthorized use of signing keys) or compromise of signature keys.

In the unlikely event that the signature key is compromised and obtained by an attacker, even if failures in the transaction function in question are fixed, the attacker can use the signature key to generate an unauthorized transaction from another node.

A flaw in the transaction-validation function would prevent the normal execution of transaction validation and confirmation. Critical vulnerabilities could also be the cause of an attack by accepting an unauthorized transaction. A large impact can cause delays or halts in the execution of transactions and smart contracts across the distributed ledger system. The impact, scope, and difficulty of fixing a flaw may be even greater if it is caused by specifications such as the transaction data format or the manner in which digital signatures are generated and verified.

3.2.2.5 Smart Contract Generation, Deployment and Execution

As described in Subsection 3.2.2.4, flaws and vulnerabilities in the set of functions involved in the generation, deployment, and execution of smart contracts can prevent their normal execution of smart contracts and, in severe cases, lead to the execution of unauthorized smart contracts. In general, the impact can extend to all smart contracts maintained by distributed ledger systems.

The magnitude and scope of the impact could be significant because smart contracts themselves may manage digital assets, such as cryptographic assets, and interact with smart contracts in other distributed ledger systems.

3.2.2.6 Node-to-Node Communication

Nodes exchange messages for transactions and distributed ledger sharing. This message exchange occurs over a communication layer, such as TCP/IP. In general, protocol and communication layer threats to message exchange include message tampering, message retransmission attacks, communication jamming, and forcing connections to unauthorized nodes.

As most distributed ledger platforms attach a node's digital signature to messages, they are considered tamper-resistant unless their signature keys and signature generation processes are weak. Communication jamming is discussed in Subsection 3.2.4.6. Some message retransmission attacks are countered by several ledger generation processes, including consensus mechanisms, based on the P2P characteristics of distributed ledger technologies.

Node communication functionality is the point of contact with nodes in the external environment with different administrators; thus, it is an easy starting point for attacks. If there is a serious vulnerability in the internode communication function of a distributed ledger platform, it may be possible to execute an arbitrary malicious code in the individual execution environment running the nodes.

3.2.2.7 Authentication and Authorization of Nodes

Node authentication and authorization functions were provided by a permission-based distributed ledger. When restricting the nodes that are allowed to connect to the distributed ledger system, or when setting up a node with privileges related to ledger generation, the node connected to the distributed ledger system is authenticated as the node itself, and the operations performed by the node are also authorized. The authentication and authorization mechanisms are provided by a distributed ledger platform. In order to actually implement authentication and authorization in a distributed ledger system, the following arrangements (collectively referred to as "operational policy") are required: determination of the entities (groups) that perform authorization, determination of the authorized nodes and authorization of operations, rules regarding the method of verifying node administrators, the method of determining such rules themselves, and determination of the entities (groups) that are responsible for such determination and implementation. An operational policy must be defined by the distributed ledger system.

Threats to the authentication and authorization of nodes include threats to the authentication and authorization mechanisms provided by the distributed-ledger platform and threats if the operational policies established by the distributed-ledger system are not properly enforced (see Section 3.5).

The occurrence of threats to the authentication and authorization mechanisms provided by the distributed-ledger platform can be attributed to the characteristics of the mechanism's specifications, flaws in its design or implementation, or a reduction in the strength of the cryptographic algorithms used and key sizes. Potential threats include node impersonation, authorization of unauthorized operations, unauthorized acquisition of ungranted privileges, and interference with specific nodes.

3.2.2.8 Cryptographic Algorithm andKey Size

Cryptographic technology plays an important role in realizing the fundamental concepts of distributed-ledger technology, such as the authenticity and verifiability of ledger data. Cryptographic technologies and application methods vary depending on the distributed-ledger platform used. Generally, they are used in the following processes:

- Digital signature
    - digital signatures on transactions
    - digital signatures on ledger data
- (Cryptographic) Hash function
    - hash trees and chains to maintain time series of transaction and ledger data
    - identifiers such as transaction and wallet addresses
    - digital signature generation process

In addition, distributed ledger platforms utilize zero-knowledge proofs and homomorphic encryption to maintain the confidentiality of transaction information primarily for security and privacy protection purposes.

The variety of cryptographic algorithms[2] employed by different distributed ledger platforms depends on the type of platform used. In addition to RSA and ECDSA, which are the most commonly used digital signatures, other algorithms, such as Schnorr signatures, are used by Bitcoin.

Cryptographic algorithms may become vulnerable in the future owing to the discovery of flaws in their design, advances in cryptanalysis, and dramatic improvements in computer performance. It is not only the algorithm itself that may be vulnerable but also the size of the encryption key[3], if they were insufficiently robust.

Although the selected algorithm and key length may be appropriate, the implementation of the algorithm may not be adequately secure, potentially rendering the implementation vulnerable to attacks. Therefore, serious vulnerabilities in digital signatures and hash functions can result in the following threats:

- Illegal transaction generation
- Incorrect ledger data generation
- Falsification (replacement) of past ledgers/transactions
    - It depends on the size and characteristics of the network of nodes.
- Unauthorized duplication of signing keys (resulting in unauthorized transaction generation)

Weak cryptographic algorithms, cryptographic keys, or implementations intended for confidentiality can result in threats that could expose information on transactions that are kept secret. The encrypted data stored in a ledger are exposed to threats from historical data.

Although each country's recommended ciphers are available as a list of cryptographic algorithms that have been evaluated for security, there are instances in which these algorithms and key lengths are not selected for use in distributed ledger platforms. In some cases, algorithms with no apparent security evaluation can be introduced. To assess the security of a distributed ledger platform, it is essential to evaluate the security of the selected cryptographic technique and methods used to implement it.

Even when the algorithm, key length, and implementation are correctly specified, inadequate management of the cryptographic key (signature key) held by a node may result in security risks, including the generation of fraudulent transactions and ledger data impersonating the node. Subsection 3.2.4. provides a detailed overview of key management for distributed ledger systems.

[2] Elliptic curve cryptography sometimes uses different curves depending on the distributed ledger platform.

[3] Cryptographic strength is determined by bit security, which relies on factors like the algorithm used (including elliptic curve parameters) and key length.

3.2.3 Threats to Distributed Ledger System

3.2.3.1 Distributed Ledger System Considerations

A distributed ledger system is composed of a network of nodes running a distributed ledger platform that is in charge of transactions and ledger processing. This subsection examines the security threats and challenges to distributed ledger systems.

- **Threats to smart contracts deployed on distributed ledgers**
- **Threats related to connections between distributed ledger systems and other systems**
- **Threats to transaction authorization and ledger generation**
- **Threats to control of distributed ledger systems**

3.2.3.2 Threats to Smart Contracts Deployed on Distributed Ledgers

Smart contracts are developed by developers who use distributed ledger systems and are deployed in the ledger data shared by the distributed ledger system.

In some circumstances, Business Zone vendors are responsible for developing smart contracts. In other instances, Business Zone vendors call contracts created by third-party developers. In some cases, a smart contract calls for the function of another smart contract. As with other cases, such as Ethereum, the smart contract itself contains a mechanism through which cryptographic and digital assets can be held and managed.

In the unlikely event that a vulnerability in a smart contract allows the smart contract process to be executed fraudulently, the worst-case scenario would be the unauthorized transfer of cryptographic or digital assets held by the user or the unauthorized transfer of cryptographic or digital assets held by the smart contract.

In addition to the potential weaknesses in individual smart contracts, there is a possibility of attacks being based on the specifications of services constructed with smart contracts.

3.2.3.3 Threats Related to Connections Between Distributed Ledger Systems and Other Systems

It is assumed that the following two interfaces will be used to connect the distributed ledger system to another system.

- **Interactive system interface—a direct connection between two or more distributed ledger systems**
- **External interfaces—connections between distributed ledger systems and external non-distributed ledger systems**

The interactive system interface is designed to connect to other ledger systems, as well as to a distributed ledger system that serves as an intermediary bridge, facilitating connections between multiple distributed ledger systems.

The external interface is designed to connect to existing centralized systems or systems that utilize nondistributed ledger technology, such as DLT Oracle (please refer to the supplemental explanation at the end of this section for more information).

In the case of a failure in the functions related to these interfaces, the connection to other systems would be interrupted, which may result in the stagnation or halt of processes executed in the distributed ledger system. Moreover, if an attacker gains access to the interface function through intrusion or malware infection of the system, there is a risk of unauthorized and illegal operations being executed on the distributed ledger system or other connected systems, including privilege escalation. In the context of an interface accessible through a network, the same threats are described in Section 3.2.2.6.

The security of other systems connected through various interfaces also influences the security of the connected distributed ledger systems. In particular, when a system is automated by smart contracts and the behavior of other systems is linked to the critical processing of the distributed ledger system, it is essential to evaluate the system with greater scrutiny. Failures in the operation of a distributed ledger system may have adverse effects such as functional halts, stagnation of connected systems or applications, or execution of unauthorized processes. Conversely, failures in connected systems or applications may adversely affect the operation of the distributed ledger systems.

When services provided by smart contracts executed by distributed ledger systems such as DeFi are interlocked, there are also attacks that exploit the discrepancies in the specifications between these services (e.g., flash loan attacks).

Supplemental Explanation of the DLT Oracle

DLT Oracle is a system that can obtain data from external sources and provide them to the distributed ledger system, or perform processing in response to events occurring in the distributed ledger system. Distributed-ledger technology enables each node to re-execute and verify the processing of a smart contract, whereas a typical distributed-ledger platform has the limitation that only deterministic smart contracts[4] can be executed. Owing to this limitation, when each node processes a smart contract, it is not possible to internally generate values other than the input values (e.g., random numbers) or process them based on information obtained directly from external resources, which may change depending on when the information is obtained. The DLT Oracle addresses this limitation by providing information about the external resources required to execute smart contracts in the distributed ledger, from external systems to the distributed ledger system. Each node of the distributed ledger system can execute smart contracts based on the values entered from the DLT oracle, which can take several forms such as a system operated by a specific administrator, a service provided by a specific entity, or a distributed system with multiple administrators.

[4] A process that will result in the same output regardless of the input values.

3.2.3.4 Threats to Transaction Authorization and Ledger Generation

The node that verifies a transaction and generates a ledger based on the results plays a fundamental role in the transaction approval process.

Several potential issues can arise with transaction authorization and ledger generation. These include software defects in nodes, attacks by malicious third parties, and operational failures. The consensus mechanism in distributed ledger technology is designed such that if a node fails, the impact of that failure can be mitigated through the work of a group of other nodes.

However, the effectiveness of the consensus mechanism may be insufficient depending on the number and deployment of nodes involved in ledger generation and approval. For example, if there are multiple nodes in a single physical location, an attack in that environment can expose them to common security risks.

3.2.3.5 Threats to Control of Distributed Ledger Systems

The specification characteristics of the consensus algorithm may enable certain user groups to assume a dominant position in a distributed ledger system or behave in a dominant manner. In addition, the generation of ledger data or the validation of transaction data may be conducted in a manner that is convenient for some users, whereas the execution of transactions or smart contracts by other users may be stalled. Moreover, transactions or smart contracts may not be executed or may be stalled during transaction execution.

In the case of a mechanism in which consensus algorithms are incentivized to acquire cryptographic assets for maintaining the distributed ledger system, a decrease in the value of cryptographic assets may reduce the incentive to participate in the distributed ledger system. This could potentially increase the risk of attackers gaining control of the distributed ledger system.Conversely, the dominant influence of a distributed ledger system on a particular group of users could result in a greater reduction in the value of the cryptographic assets provided by the distributed ledger.

3.2.4 Threats to Systems in Business Zone Connected to Distributed Ledger System

3.2.4.1 Business Zone System Considerations

This subsection discusses security threats and issues common to Models 1 through 3 for the Business Zone systems connected to distributed ledger systems. The following items are included.

- **Threats to the execution environment of distributed ledger nodes**
- **Threats to key management in distributed ledger nodes**
- **Threats related to connection to distributed ledger applications**
- **Threats of ledger inconsistency due to specification changes in distributed ledger platforms**
- **Denial of Service (DoS) threats to distributed ledger systems**

3.2.4.2 Threats to Execution Environment of Distributed Ledger Nodes

A malicious actor or malware infection of the environment, such as a device running each node that comprises the distributed ledger system, can result in unauthorized execution, shutdown, or configuration changes in the node's functions without authorization.

Such an incident can result in unauthorized access to signature keys or the leaking of keys managed by the node. It can also lead to tampering with transactions or smart contracts before they are signed, disabling node functions such as transaction and ledger validation, interfering with message forwarding to other nodes, and sending unauthorized messages.

The impact of a particular node's abnormal behavior on the distributed ledger system as a whole is contingent on the size of the node's network and the importance of that node's role within the system. If a node performs a significant verification function within the distributed ledger system, the impact is more pronounced.

In addition to posing a risk to distributed ledger systems, malware infection of the execution environment can lead to unauthorized control of the device, potentially enabling its use in attacks against other devices and systems in the network.

It is important to consider not only malicious external actors but also the possibility of internal fraud within the organization that manages the node.

3.2.4.3 Threats to Key Management in Distributed Ledger Nodes

Each node in a distributed ledger system is responsible for managing the signature key to generate digital signatures for transactions and ledger data. Digital signatures used to generate transactions are necessary components of the transfer process for digital assets. Numerous nodes participating in a distributed ledger system manage their own signature keys.

It is crucial to ensure that the signature key used for ledger data generation is reliable and authentic. Each node responsible for ledger data generation manages its own signature keys.

Unauthorized access to a signature key can result in the generation of unauthorized transactions or ledger data by a malicious actor, which can have significant financial implications. Furthermore, the compromise of a signature key through the network or the theft of the physical medium on which the signature key is stored allows another node in the distributed ledger system network to utilize that signature key. Therefore, the potential damage caused by the compromise or theft of a signature key cannot be mitigated by simply disabling the functionality of the node that has been attacked.

When an unauthorized transaction is detected in a standard distributed ledger system, particularly in a public permissionless type, the impact of threats of unauthorized access to or compromise or theft of signature keys is significant. This is because transactions cannot be rolled back or revoked in the system after being approved by a ledger.

It is important to consider not only external malicious actors but also the potential for internal fraud, unauthorized use, leakage, or theft of signature keys within the organizations that manage them.

3.2.4.4 Threats Related to the Connection to Distributed Ledger Applications

In this discussion, we assume the following two connection interfaces for distributed ledger applications:

- User interface - connection between the user application and distributed ledger system
- Administrative interface - connection between the administrative application and the distributed ledger system

The user interface acts as an intermediary between the distributed ledger system and user. It connects to a user application that oversees the transaction operations of the digital assets managed by the distributed ledger system, oversees the digital signature keys, and handles the transaction generation process. User applications can be provided in desktop, web, mobile, and console command-line formats.

The administrative interface offers operational capabilities for node management. It provides functions for node configuration, startup, shutdown, connection to other nodes, the management of distributed ledger data, etc.

If the functions associated with these interfaces fail, the connection to the application is disrupted, causing the processes within the distributed ledger system to come to a halt.

Furthermore, if the interface function is exploited by a malicious actor or malware infection in the system that provides the interface function, there is a risk of unauthorized operations in the distributed ledger system or applications connected to the interface, or of unauthorized privilege escalation. If the interface is accessible via a network, the risks described in Subsection 3.2.2.6 “Node-to-Node Communication” may arise.

Defects or vulnerabilities in either the interface or the connecting application can result in the same threats as previously described. It is important to note that the management application and interface have the capability to perform privileged operations in the distributed ledger system and nodes.

3.2.4.5 Ledger Inconsistency Due to Changes in Distributed Ledger Platform Specifications

It is crucial to highlight that in the event of changing specifications for distributed ledger platforms, it is essential to consider the implications of hard forks that necessitate updating all nodes and applications connected to the distributed ledger system. Because of the split in the ledger that occurs with a hard fork, if no update is made, the previous ledger data will be left behind, resulting in incorrect processing of transactions. It is crucial to pay close attention to public permissionless distributed ledgers because they are responsible for responding to specification changes.

3.2.4.6 DoS Threats to Distributed Ledger Systems

If a node, system, or application connected to a distributed ledger system generates a large number of requests or other communications to a specific node that exceed its processing capacity, this can affect the normal processing of that specific node.

If a node managed by the Business Zone system becomes the target of an attack, the normal execution of the services provided by the system will be disrupted. Furthermore, the disruption of the normal reception of ledger data from other nodes may result in potential threats, including the possibility of intentional ledger splitting (chain splitting) at the attack target node or a double spending attack on digital assets. A DoS attack may occur at the communication layer such as TCP/IP or at the level of the distributed ledger protocol implemented before it.

3.3 Security issues Related to Anticipated System Model 1 (Public Permissionless with Custodial Wallet Type)

System Model 1 is designed to facilitate the management of signature keys essential for the transfer of digital assets within the Business Zone system. In this model, it is essential to manage the correspondence between end users who have rights to digital assets, the digital assets (signature keys) in themselves, and the digital currency platform accounts in the Business Zone system. The following issues regarding these controls are addressed:

- **Identity proofing and authentication of the end user**
  To prevent end-user identity theft, maintain normal services, and prevent the transfer of criminal proceeds and other social responsibilities, it is necessary to verify the identity of end users and provide appropriate means of authentication when providing services. If the authentication process for providing service functions related to digital assets is inadequate or vulnerable, threats such as end-user impersonation or unauthorized privilege escalation may occur.

- **System-wide security issues in the Business Zone**
  As with any general system, the entire Business Zone system must be prepared for a range of potential threats, including cyberattacks, physical attacks on the devices and facilities running the system, and insider threats. The Business Zone systems in System Model 1 are subject to several challenges, including the following:
  - **Threats to the distributed ledger platform deployed and connected distributed ledger system**
    It is essential to prepare for the risks associated with defects and vulnerabilities in distributed ledger platforms and distributed ledger system incidents, as detailed in Section 3.2. Especially in the case of public permissionless distributed ledger systems, it is important to assume that there could be threats that cannot be controlled from the Business Zone systems.

- **Signature keys for digital currency**
  In the event of the unauthorized use, compromise, or theft of signature keys utilized to connect to digital currency platforms, an unauthorized transfer of digital currency could occur. Although digital currency platforms are equipped with anti-abuse mechanisms, it is essential to implement proper signature key management in each Business Zone system to ensure that these measures are effective. For further details on signature key management, see Subsection 4.4.3 “Key Management for Distributed Ledger Nodes."

- **Signature keys on digital assets**
  It is important to note that the unauthorized use, compromise, or theft of signature keys related to digital assets can cause significant damage, with the potential for a greater impact on digital assets of higher value. To mitigate the risks outlined in Subsection 3.2.4, a robust key management strategy must be deployed for digital assets to which end users and Business Zone vendors have authorized access.

- **Digital asset and end-user management**
  To protect the rights of end users’ digital assets, it is essential to properly management the correspondence between these entities. Inconsistencies in the management of this correspondence, whether owing to improper operations, operational errors, external attacks, or internal fraud, result in the loss of end users’ assets.

3.4 Security Issues Related to Anticipated System Model 2 (Public Permissionless with Non-Custodial Wallet Type)

In System Model 2, digital asset wallets prepared by end users are linked to digital currencies managed by digital currency platforms. It is essential to maintain transaction consistency between the digital assets managed by the digital asset wallet and the digital currency in this model. The following issues are addressed:

- **Risks of digital asset wallets**
  Many forms of digital asset management wallets exist, including desktop software, mobile applications, third-party key management services, and hardware solutions. Significant vulnerabilities in digital asset wallets can result in loss of digital assets.
  Moreover, if digital currency transfers are conducted through digital asset wallets, there is a risk of damage to the digital currency. Because digital asset wallets are provided by third parties that are not involved in the digital currency platform, exerting direct control over their quality is not straightforward.

- **Identity proofing and authentication of the end user**
  As with Model 1 in Section 3.3, it is essential to verify the identity of end users correctly when providing services and to provide appropriate authentication methods for end users. When utilizing authentication methods for digital asset wallets provided by third parties, it is important to assess the security of the authentication methods.

- **Binding of digital asset wallets to user accounts**
  The system must verify that the user is a legitimate account holder of a digital asset wallet and manage the binding of the digital asset wallet to the Business Zone's service account and the digital currency account. Vulnerabilities in this binding process could result in unauthorized digital asset wallets or unauthorized users being bound, leading to the loss of digital assets, unauthorized transactions of digital assets (e.g., the transfer of criminal proceeds bypassing surveillance), and unauthorized transfer of digital currency.

- **Digital asset wallet migration**
  A change in the digital asset wallet to another form or migration of the device on which it is running to another device will occur. Potential vulnerabilities in the process of these migrations could result in the digital asset wallet being bound to another unintended user or device, which could lead to the loss of digital assets or an unauthorized transfer of digital currency.

- **Digital asset transfer operations**
  In the example flow of this model, brokerage of the transfer of digital assets between end users is performed using smart contracts deployed in a distributed ledger system. If the smart contract is vulnerable, there is a risk of unauthorized manipulation of digital assets. In severe cases, this can result in the leakage or loss of digital assets managed by the smart contract.

  If smart contracts are not utilized in a manner described in the previously outlined example, a mechanism will be established to ensure the integrity of digital asset transfers and currency payments within the Business Zone system. It is essential to maintain the integrity of the digital asset transfer process performed by the end user in the distributed ledger system using the digital asset wallet and digital currency transfer performed using the digital currency wallet. Inconsistencies in either process can result in a loss of digital assets and currency. Furthermore, vulnerability in this process can result in the theft of digital assets and currency by malicious actors.

- **Monitoring of digital asset transactions**
  Although the transfer of digital assets is performed by the end users, the Business Zone services who act as intermediaries for the transactions are accountable for the series of transactions to a certain extent. From a social responsibility perspective, monitoring digital asset transfers may be necessary to prevent the transfer of criminal proceeds.

3.4 Security Issues Related to Anticipated System Model 2 (Public Permissionless with Non-Custodial Wallet Type)

- **System-wide security issues in the Business Zone**
  As is the case with general systems, the entire Business Zone system must be prepared for cyberattacks, physical attacks on the devices and facilities running the system, and insider threats. The issues in the Business Zone systems in Model 2 include the following:

  - **Signature keys for digital currency**
    As with Model 1, it is essential to properly manage the signature keys for connections to digital currency platforms. For guidance on the management of signature keys related to digital currency platforms, please also see Subsection 4.4.3 "Key Management for Distributed Ledger Nodes" for further information on signature key management.

  - **Digital asset information and end-user management**
    This system is responsible for managing information pertaining to end users and the content of digital assets managed by the end users. Inconsistencies in the management of this correspondence owing to improper operations, operational errors, external attacks, internal fraud, or other reasons will prevent the proper execution of digital asset transactions and harm end users and Business Zone systems.

3.5 Security Issues Related to Anticipated System Model 3 (Private Permissioned)

In Model 3, the Business Zone system manages the signature keys required to transfer the digital assets. This model is similar to Model 1 in that it manages digital assets (signature keys) and end users with rights to digital assets in the Business Zone system. Model 3 presents the following issues:

- **Identity proofing and authentication of the end user**
  As in Model 1, there are risks associated with impersonation and unauthorized privilege escalation in the process of identifying end users for service implementation and in the provision of authentication mechanisms.

- **System-wide security issue in the Business Zone**
  To mitigate risk, the entire Business Zone system must be prepared for a range of potential threats, including cyberattacks, physical attacks on the devices and facilities running the system, and insider threats. The Business Zone systems in Model 3 present several issues, including the following:

    - **Threats to the distributed ledger platform and connected distributed ledger system**
      It is essential to anticipate and prepare for potential risks associated with distributed ledger platform defects, vulnerabilities, and distributed ledger system incidents, as outlined in Section 3.2. In a private permission distributed ledger, a node with the privilege of generating ledgers and approving transactions (privileged node) can be predetermined and operated. Furthermore, distributed ledger platforms may be designed for such operations, with the responsibility of a particular node often exceeding that of a public permissionless node. It is important to ensure that multiple privileged nodes are appropriately distributed and operated.

    - **Signature keys for digital currency**
      As with Model 1, it is important to ensure the proper management of signature keys for connections to digital currency platforms. For further information on signature key management, please refer to Subsection 4.4.3 "Key Management for Distributed Ledger Nodes."

    - **Signature keys on digital assets**
      The unauthorized use, compromise, or theft of signature keys related to digital assets can cause significant damage, with the potential for greater losses associated with digital assets of higher value. Furthermore, the Business Zone system necessitates stringent control over the signature keys for authentication and authorization to connect to the distributed ledger system. In addition, the signature keys required for operations when the system assumes the role of a privileged node involved in ledger generation and transaction approval must be strictly managed. The unauthorized use, compromise, or theft of signature keys can result in unauthorized ledger use, ledger generation, and transaction approval. These incidents can affect the entire distributed ledger system.

    - **Digital asset and end-user management**
      To safeguard the interests of end users with regard to their digital assets, it is essential to ensure effective management of the relationship between end users and their digital assets. Inconsistencies in the management of this correspondence, whether owing to improper operations, operational errors, external attacks, or internal fraud, result in the loss of end users' assets.

- **Examination related to the connection of the distributed ledger system**
  Private permissioned distributed ledger systems require authentication and authorization for nodes, systems, applications, and users seeking to establish connections. As a prerequisite for authentication and authorization, a prior examination of connected systems, management entities, and so forth, is required. If the screening criteria or implementation methods are inadequate, connections to inappropriate systems or applications, or connections from unauthorized users may be permitted, which could result in risks such as unauthorized manipulation of the distributed ledger system or contamination of ledger data.

Addressing Security Issues

04

CONTENTS

The Digital Currency Forum
Wallet Security Subcommittee

Chapter 4

Addressing Security Issues

4.1 Introduction

This chapter examines the potential countermeasures, mitigation strategies, and response policies for the security concerns addressed in Chapter 3.

4.2 Addressing Issues Related to Distributed Ledger Platforms and Distributed Ledger Systems

The security of distributed ledger platforms and distributed ledger systems is evaluated from the following perspectives:

- Evaluation of distributed ledger platform design and specifications
- Evaluation of distributed ledger platform implementations
- Evaluation of distributed ledger systems

Evaluating the design, specifications, and implementation of distributed ledger platforms and assessing distributed ledger systems are currently challenging. As discussed below, it may not be realistic for Business Zone service providers to conduct this evaluation individually. It is necessary to mitigate the risk given that evaluation is difficult.

To evaluate the security of a distributed ledger platform, it is essential to assess the security of its functions, elements, and combinations of these elements.

As described in Subsection 3.2.2.1, these include functions and elements such as consensus mechanisms, transaction generation and verification methods, smart contract generation and deployment methods, inter-node communication, node authentication and authorization, and cryptographic algorithms. It is important to note that each distributed ledger platform employs its own consensus mechanism, different cryptographic algorithms, and so forth. Consequently, each platform must be evaluated according to its architecture.

As some consensus mechanisms work in conjunction with incentives such as rewards to encourage cooperation and competition among nodes, thereby ensuring that the ledger is unique to each node, it may also be necessary to evaluate the design of the incentives. The various mechanisms underlying distributed ledger platforms, including consensus mechanisms, have not always been assessed for safety in academic research. Furthermore, distributed ledger platforms comprise numerous technical components that make their implementation a complex process.

Given the diverse range of functions offered by distributed ledger platforms, there is currently no unified set of evaluation criteria within the distributed ledger field. It is essential to conduct a thorough evaluation of the implementation codes of the individual distributed ledger platforms. Frequent changes in the specifications of distributed ledger platforms also represent a challenge in the evaluation process.

The evaluation of a distributed ledger platform as secure does not guarantee that the system running on the platform is secure. As noted in Subsections 3.2.3 and 3.2.4, if the number and configuration of nodes, or the management of signature keys, as assumed by the distributed ledger platform, do not align with expectations, the security of the distributed ledger system may be at risk.

In particular, as observed in public permissionless distributed ledgers, it is sometimes difficult to grasp the actual network configuration. This can result in discrepancies between the actual situation and assumptions made when designing a distributed ledger platform. It is essential to gain a clear understanding of the actual distributed ledger system situation and the cases that may arise.

In the case of a distributed ledger like Bitcoin, where the value of the cryptographic assets issued by the system can affect the security of the distributed ledger, it is important to monitor the value of these assets and the nodes responsible for generating the ledger.

For private permission distributed ledgers, the number of connected nodes is limited, and a certain degree of control over node operations is possible. The architecture of the distributed ledger platform is designed considering these factors. Along with the security features of the distributed ledger platform, which are described above, it is important to consider the nodes that comprise the distributed ledger system. In particular, the number and configuration of the nodes involved in ledger generation and transaction approval, management entities, and management and operation methods should be considered. For the private permissive types, please see Section 4.7 for further details.

4.2 Addressing Issues Related to Distributed Ledger Platforms and Distributed Ledger Systems

Although it would be beneficial to assess the security measures of distributed ledger platforms in terms of their design, specifications, implementation, and distributed ledger systems, there is no uniform standard for distributed ledger platforms. It is challenging to evaluate the safety of individual distributed ledger platforms and distributed ledger systems as a whole, rather than as individual functional elements. It is expected that an evaluation method will be established in the future through collaboration among academia, industry, and standardization organizations involved in distributed ledgers, to enhance their knowledge.

Conversely, Business Zone service providers must acknowledge the potential risks associated with distributed ledger platforms and distributed ledger systems. To mitigate these risks and ensure business continuity in the event of an incident, service providers should consider implementing measures that address the following aspects:

- **Gathering and evaluating information on distributed ledger platforms and distributed ledger systems**
  It is essential that vendors gather information about distributed ledger platforms and distributed ledger systems to have a comprehensive understanding of the technology, digital assets being handled, and potential risks. Furthermore, the deployment of a distributed ledger platform may necessitate an assessment of the platform, Layer 2 software, and wallet implementations. This evaluation may also require third-party source code audits and similar procedures.

- **Gathering information about the distributed ledger platform development community**
  It is essential to understand the composition of the development community, how it makes decisions, how it engages in specification changes, and its relationships with other communities. In some cases, it is necessary to note the developers and operators who influence specification changes for distributed ledger platforms, as well as the governance token holders and their trends.

- **Understanding the latest trends in distributed ledger platforms and distributed ledger systems**
  It is essential to identify and address any changes in specifications, bug fixes, vulnerability fixes, and large-scale migration plans. Furthermore, it is important to consider the impact on wallets, applications, and systems connected to the distributed ledger system, as well as the impact on smart contracts running on the distributed ledger system.

- **Monitoring distributed ledger systems**
  Monitoring the status of distributed ledger systems in real time is crucial. In the case of an anomaly, this issue must be analyzed and resolved. If there is suspicion of irregularity in a specific node, monitoring may be conducted on multiple nodes with different connection points.

- **Updating distributed ledger nodes**
  In the event of updates to a distributed ledger platform, whether for specification changes, bug fixes, or vulnerability fixes, node updates are considered and implemented according to the requirements of the update content.

- **Establishing a response system and studying and implementing response measures**
  It is essential to establish a response system for distributed ledger issues that incorporates the above perspectives and considers the best approach for addressing potential risks. This includes contingency plans for addressing anomalies in the distributed ledger system in response to identified threats, as well as plans for managing the impact of large-scale migration. When developing specific measures, it is essential to seek input from experts with knowledge of distributed ledger systems.

4.3 Development of Business Zone Systems

4.3.1 Fundamental Policy

In addition to the system development that is already familiar to us, Business Zone systems require the development of smart contracts and distributed ledger applications. When developing Business Zone systems, it is essential to ensure that the design and development are secure and based on the characteristics of the distributed ledger platform and system to be employed, as well as the potential threats to Business Zone systems (see Section 3.2). The next subsection will discuss the fundamental concepts of risk mitigation for smart contracts.

4.3.2 Smart Contract Risk Mitigation

Similar to general software, the process of developing smart contracts requires a structured approach that includes secure design, detailed specification reviews, secure coding practices, code reviews, test designs, and test executions.

The design of the smart contract includes the design of the authorization to execute each function. Smart contracts may include restrictions specific to smart contracts in general programming languages or introduce languages designed specifically for smart contracts. Those working on the design, review, coding, or testing of smart contracts should understand the language specifications of smart contracts adopted by distributed ledger platforms. Participation in a smart contract developer community is widely acknowledged as an effective way of acquiring knowledge. Some languages for developing smart contracts with a large number of developers provide a summary of vulnerabilities, items to consider in secure programming, vulnerability testing tools, etc. This information could be helpful as a reference for developers.

For reviews, it is advisable to engage a knowledgeable and experienced third party to conduct a smart contract audit or vulnerability assessment. A review of the specifications and codes of any smart contracts provided by a third party with expertise is recommended whenever possible.

The environment of the virtual machine executing the smart contract may be updated to include vulnerability support to enhance security. It should be noted that older versions of smart contract codes may not be compatible with updated virtual machines. Failure to update the virtual machine and reuse old codes containing vulnerabilities can result in security issues. New developments should utilize the latest virtual machines and use functions that have been corrected for vulnerabilities. Furthermore, when maintaining smart contracts, it is crucial to update the virtual machine to address vulnerabilities, update smart contracts accordingly, and prohibit the reuse of old code that contains vulnerabilities.

Smart contracts must be updated even after deployment on a distributed ledger to address any defects discovered during operation. It is essential to ensure that the functionality of these contracts is not misused or modified by third parties without authorization.

Smart contracts must be carefully tested before deployment in a distributed ledger. Smart contracts can be tested in a local environment without being deployed in a distributed ledger. However, it is also necessary to test them in a distributed ledger system consisting of multiple nodes. A test environment for smart contracts could be a network for testing that is publicly available for development or a private distributed ledger that one has built.

In addition, it is desirable to consider risk mitigation and risk transfer measures, such as operational measures and insurance, in the event of a smart contract failure.

4.4 Security Measures for Business Zone Systems

4.4.1 Information Security Management

In addition to general information security management, as typified by ISO 27001 and ISO 27002, the Business Zone system may establish and implement a security structure that addresses the risks specific to distributed ledgers, as discussed in Section 4.2.

Management should conduct a risk assessment of Business Zone systems based on the characteristics of the distributed ledger platform and distributed ledger system and the assumed threats. Based on the responses to the distributed ledger questions in Section 4.2, the aim is to establish an overall structure and policies for the security of Business Zone systems. In addition, an appropriate access control system is designed and implemented, and a structure for network and system monitoring, incident response, vulnerability response, etc. is established. Countermeasures are implemented simultaneously.

The system model presented in Chapter 2 provides an example of an NFT; however, Business Zone systems may be capable of handling other digital assets. In accordance with the specific characteristics of the digital assets involved, Business Zone service providers may be required to comply with the applicable laws and regulations. If industry-specific or regulatory standards for security are in place, Business Zone systems must comply with these standards.

4.4.2 Security Measures for Distributed Ledger Nodes

As with other elements of the Business Zone system, cybersecurity measures must be implemented to protect against unauthorized access and malware in the execution environments of the ledger nodes. Given that distributed ledger nodes connect to external nodes and are vulnerable to external attacks, they must be separated from the backbone of a Business Zone system. Furthermore, the network must be monitored to detect abnormalities.

It is also advisable to limit the number of functions that can be performed in a distributed ledger node environment. It may be feasible to separate the node environment that only refers to the distributed ledger from the one that performs the transaction transmission.

Furthermore, it is essential to verify the operational status of the blockchain nodes managed in the Business Zone and external blockchain nodes. For example, it is essential to confirm block generation, MemPool updates, and so forth. It is also important to block unnecessary communication by limiting the number of connection points from the node environment, including measures against DoS attacks. As a further precaution against tampering with messages not subject to signatures, eavesdropping, and connections to unauthorized nodes, it is recommended that secure communication such as Transport Layer Security between nodes be configured, if applicable.

To maintain the integrity of the distributed ledger and mitigate risks such as the failure of specific nodes, a monitoring solution that involves multiple nodes in different networks can be implemented.

In Business Zone systems, when a distributed ledger system is connected and linked to other systems (including DLT oracles and non-distributed ledger systems) and applications, the operations that can be performed, messages sent on both sides between systems and applications, authorization required to perform operations and send messages, and mechanisms such as authentication and authorization must be appropriately designed and implemented. Moreover, evaluations and audits of the DLT oracle and other systems to be connected should be conducted as required.

4.4.3 Key Management for Distributed Ledger Nodes

Distributed ledger nodes are responsible for managing the signature keys to generate transactions. Furthermore, if they are responsible for transaction approval or distributed ledger generation in a distributed ledger system, they must manage the required signature keys. Any unauthorized access to or compromise or theft of signature keys required for transaction authorization or distributed ledger generation will significantly impact the entire distributed ledger system. Therefore, it is essential to pay greater attention to these security issues.

In a distributed ledger, different types of signature keys exist, such as the signature key used to sign transactions (transaction signature) and the signature key used to approve transactions and ledger data (block signature). In particular, the unauthorized use of a privileged signature key related to approving transactions or ledger data or configuring the distributed ledger system or smart contracts will have an impact on the users involved in the distributed ledger system and the system as a whole. Privileged signature keys must be managed with greater care.

The specific type and nature of the signature key in use should be identified, and its lifecycle should be clearly defined. For a distributed ledger system that manages digital assets, it is important to consider the value or amount of digital assets managed by the signature key. Given the varying degrees of risk associated with different types of signature keys and the value of the digital assets they handle, it is essential to consider an appropriate level of key management in line with the level of risk. The life cycle of a signature key includes the following stages: generation, activation, deactivation, suspension, and disposal. Activation is the process of moving a signature key from a protected state to a state in which it is available for use. The opposite is true for deactivation. When defining the lifecycle of a signature key and establishing an operational policy for a signature key, it is essential to consider the digital assets associated with it. For a distributed ledger that manages digital assets, the generation of a new signature key may involve the transfer of digital assets to that signature key. Furthermore, when an old signature key is disposed of, the option of subsequently transferring digital assets to that signature key should also be considered.

The objective is to design a signature key management system that can effectively manage signature keys based on their specific characteristics. Implementing appropriate access controls in signature key management systems is essential to prevent leakage or unauthorized access to signature keys. The signature key management system must ensure that other modules or systems do not have direct access to the signature key data. For instance, the signature key management system should ensure secure management of the signature key and provide only an interface that receives requests for signature generation and returns signature values.

If the transaction data sent to a signature key management system are incorrect, there is a risk that the signature key management system will perform the signing process for that transaction. To mitigate this risk, it is essential to validate the legitimacy of the transaction data prior to their transmission to the signature key management system. For instance, it may be advisable to confirm that the transaction is directed toward a pre-registered recipient (white list) or to identify irregularities based on historical data such as the amount of money involved in the transaction. It is important to note that these risk mitigation measures should be considered separately from the signature key management systems.

To guarantee strict control of signature keys, it may be necessary to deploy an evaluated hardware security module (HSM). It is possible that the signature algorithm utilized by a distributed ledger platform will not fall within the scope of certification standards such as FIPS (CMVP) or Common Criteria. In such cases, implementing a mechanism to protect the signing keys in the HSM is an effective way to ensure proper key management. If a module or system containing a signature key operates on a physical device, measures must be implemented to protect it from physical destruction or theft. It is advisable to install the module or system in a physically protected module or robust facility and implement physical access controls such as access control. Furthermore, it is essential to maintain strict control over authentication credentials when user authorization is conducted on modules or terminals associated with signature key management systems.

4.4.3 Key Management for Distributed Ledger Nodes

The operational policy for the signature key management system is developed in accordance with the information security management guidelines and policies for the entire information system, including the signature key management system. The operational policy for the signature key management system establishes the key management system and defines the roles and authorities associated with key management. For instance, the key management supervisor bears the responsibility for signature key management, the administrator oversees the site, the operator performs operations related to signature key management in accordance with regulations, and the auditor conducts audits. It is recommended that personnel do not have multiple roles that would constitute a conflict of interest and that personnel be changed as necessary to avoid a concentration of authority in any individual. Furthermore, mutual monitoring by two or more operators and approval by a manager or responsible individual are essential to prevent internal fraud and operational errors in certain critical processes. Moreover, the records of all key-related operations must be maintained, and any irregularities should be monitored and audited retrospectively. It is also essential to establish clear guidelines in advance for reporting and addressing irregularities.

It is also essential to define the backup, restore, and archive operational policies as part of the operational policy. It is advisable to back up the signature keys in the event of a loss. However, backup management must be subject to the same rigorous controls outlined previously. To prevent unauthorized access to signature keys due to theft, leakage, or unauthorized manipulation of backup data, the following aspects of the backup and restoration process should be clearly defined and properly implemented: backup data creation and storage, restoration (restore) methods and procedures from backup data, operator authority settings, and access control.

To mitigate the risks of unauthorized access, leakage, or theft and to ensure availability in case of failure, digital asset management signature keys can be divided into multiple keys and managed in different locations. Some distributed ledger platforms are equipped with functions such as the multi-signature function, which can be operated using multiple signature keys. These functions can be utilized as required. Some smart contracts offer the same functionality as multi-signature systems, but it is important to evaluate smart contracts from a security perspective. It is possible to divide the signature key into multiple shares using secret sharing or other means, without using functions supported by distributed ledger platforms or smart contracts. However, the security of the algorithm must also be considered. If management is conducted using multiple signature keys, insecure keys resulting from inadequate management may become susceptible to attacks. Although the unauthorized use of some signature keys does not immediately result in the unauthorized use of digital assets, it diminishes the overall security of the entire set of signature keys that comprise the same set of unauthorized keys. The benefit of splitting a signature key into multiple keys cannot be realized if the signature key management is inadequate. All the multiple keys should operate in accordance with the same security level. Regarding the backup of multiple keys in the event of a failure of a signature key, the backup must be managed in accordance with the same standard as the signature key in operation.

When individual signature keys are generated from a master signature key or seed, the master signature key or seed must be managed with the same or higher standards as those applied to individual signature keys. For cryptographic keys that are used for confidentiality or other purposes and are not signature keys, the key management system should be established and implemented according to the aforementioned policy, considering the specific type and life cycle of the key in question.

In the unlikely scenario in which an anomaly is detected in the operation of a signature key, leading to the suspicion of unauthorized use, it is imperative that a new signature key is generated and the digital assets are promptly transferred to the address corresponding to the new signature key. This is particularly crucial in the context of public permissionless distributed ledgers. Because the system module responsible for generating signature keys may be susceptible to manipulation by malicious actors, it is crucial to ensure that the generation and transmission of transactions for new signature keys and digital asset transfers are conducted in a secure and uncompromised environment.

4.5 Responding to Security Issues for Model 1

- **End-user identity proofing and authentication**

  In this model, Business Zone service providers act as the custodians of digital assets. Therefore, it is vital to ensure proper identification of end users to protect consumers and prevent the transfer of criminal proceeds.

  Standards for identity proofing process vary depending on the nature of the digital assets involved. These may include the requirements set forth by the Act on the Prevention of Transfer of Criminal Proceeds, industry-defined standards, or NIST SP800-63-3 (63A)[5] as a standard for general identity proofing. Identity proofing process must be conducted at the time of service initiation (onboarding) and on an ongoing basis, depending on the transaction risk. In the identity proofing process, it is essential to ensure that no unnecessary information is obtained or stored, to protect the privacy of end users.

  It is essential to implement authentication methods to verify that end users can control their authenticators when accessing services provided by Business Zone systems and executing transactions[6] involving digital assets. In particular, the execution of digital asset transactions requires highly secure means such as the introduction of appropriate multi-factor authentication. The NIST SP800-63-3 (63B) standard defines the general level of authenticators.

- **System-wide security measures for the Business Zone**

  As discussed in Sections 4.2–4.4, security management of the systems in the Business Zone is necessary based on the characteristics of the connected distributed ledger systems. It is crucial to monitor incidents in public permissionless distributed ledgers as well as trends in vulnerability discovery and specification changes. If a significant issue occurs with the distributed ledger that could potentially impact the Business Zone system, it will be necessary to disconnect the link to the distributed ledger system. Some types of threats, such as those targeting signature keys used for transferring digital assets (see Subsection 3.2.4.3), cannot be mitigated simply by disconnecting the link to the distributed ledger system. To prepare for such incidents, it is necessary to consider the possibility and implementation of transferring and protecting digital assets in advance and define the response methods to be used.

  Furthermore, to safeguard end users' digital assets, it may be advisable to implement measures for the appropriate segregation and management of end users' digital assets and signature keys, which are essential for the transfer of digital assets. It is important to keep records of the processes and operations performed on systems in the Business Zone to immediately detect and respond to anomalies, discover and identify the causes of anomalies through subsequent audits, and enhance security. These records should include appropriate information for these purposes.

- **Confirmation of transaction**
  Business Zone service providers are obliged to identify and mitigate the risks of digital asset transactions used for the transfer of criminal proceeds and other illicit activities. In accordance with the level of risk and necessity, it is essential to obtain information on the purpose of digital asset transactions and the destination of digital assets from end users. This information should be recorded to detect suspicious transactions.

[5] The document is currently being revised as SP800-63-4, with a draft version now available.。
[6] The authentication method for digital currency payments is provided by the digital currency platform,

4.6 Responding to Security Issues for Model 2

- **Clarification of the scope of responsibility assumed by Business Zone service providers**
  The scope of liability and guarantees that the Business Zone service provider assumes regarding damages caused by problems with digital asset wallets controlled by end users should be determined and clearly communicated to the end users. The damage includes those related to Business Zone services, end users' digital assets, and digital currency. Even when presented with digital asset wallets that are technically connected to the Business Zone system, end users may misinterpret these wallets as endorsed and secured by the Business Zone service provider. Business Zone service providers are expected to provide mechanisms and appropriate guidance to end users to protect their digital assets and currency properly within the scope of their responsibilities.

- **End-user identification and identity proofing process, binding to a wallet**
  To fulfill their responsibility as intermediaries in transactions, Business Zone service providers must identity proofing process on end users, as in Model 1. In addition to identity proofing process, confirmation that the end user has control of the wallet and binding the end user's information to the wallet's information are required . This process requires confirmation that the end user is in control of their wallets. The method of binding the end user's information to the wallet varies depending on the type of wallet, but includes a process such as verifying the digital signature provided by the end user and comparing it to the information presented by the Business Zone system. Because there is a risk that this process could force end users to sign unintended transactions, it is undesirable to use signature keys for this process, which can actually transfer digital assets.

  Wallets whose signature keys are tightly controlled by hardware may achieve a higher level of binding security, whereas other wallets may require a more careful assessment of threats and risks in the binding process.

  End users are responsible for managing credentials for authentication to wallets and for signature generation (activation of signature keys). Moreover, if end users are required to manage authentication credentials to access services provided by the Business Zone system, this will result in an increased administrative burden on end users. To reduce this burden, it is important to exercise caution when using the authentication mechanism of a wallet as a means of authenticating services provided by a Business Zone system. Considering binding, the use of signature keys for transferring digital assets as a means of authentication should be avoided. The authentication means provided by the wallets must meet the appropriate strength criteria, and the authentication means must be provided separately from the signature on the transaction. When considering identity federation with an online wallet service using the wallet service's authentication means, it is necessary to ensure that the trust framework, including the identity proofing process method of the wallet service and authentication means at the time of account registration, meets the required standards for the services provided by Business Zone systems.

- **Evaluation of corresponding wallets**

  The following aspects are used to evaluate the security of digital asset wallets:

    - Implementation types for digital asset wallets (e.g., software, hardware, service)
    - Security measures for digital asset wallets

    It includes the following items:
        - Methods for signature key generation
          Algorithms for signature key generation and methods for generating random numbers are used for signature key generation.
        - Managing signature keys
          Where signature keys are stored, how operations are conducted on signature keys, whether and how signature keys can be imported or exported, whether and how signature keys can be backed up or duplicated, and how encryption key are managed, if applicable.
        - Authentication and authorization methods for operations on digital asset wallets and signing keys
        - Security measures for digital asset wallet interfaces
        - Physical protection for digital asset wallets
        - In the case of service-type wallets, it includes the following:
            - Digital asset wallet providers, security management, cyber and physical security measures for systems

    - Scope of third-party evaluation, if any, for the above
      Only some of the functions or elements in the examples above may be subject to evaluation. Although it would be optimal for businesses to evaluate the security of digital asset wallets connected to Business Zone systems in advance, it may be challenging for individual businesses to do so. Industry groups and organizations for standardization are expected to establish evaluation criteria for digital asset wallets in the future. These criteria will be used to evaluate the security of digital asset wallets, and the results will be shared.

4.6 Responding to Security Issues for Model 2

- **Digital asset wallet migration**
  During the process of migrating to different digital asset wallets or migrating devices with digital currency wallets installed, etc., it is essential to take preventive measures to ensure that users, devices, and wallets are not tied to unintended users, devices, or wallets. In instances where the constraints of wallets or devices may impede the consistency of the migration process, the end-user identity proofing process and binding processes may be re-initiated.

- **System-wide security measures for the Business Zone**
  It is essential to implement a security management system for the Business Zone systems that align with the specific characteristics of the distributed ledger system being connected. The fundamental concept is consistent with that of Model 1. However, the following points require attention.

- **Maintaining the integrity of transactions with digital assets and currencies**
  As digital assets are transferred via digital asset wallets under end-user control, it is necessary to verify the distributed ledger that manages these assets and ensure consistency with digital currency transactions conducted in the Business Zone system. If end-user transfers of digital assets are not completed, appropriate measures, including the suspension of digital currency transfers or the issuance of refunds, will be implemented. Considering the potential for the distributed ledger to be rolled back, it is essential to conduct periodic checks on the information stored in the ledger to ensure the integrity of the digital asset data managed by the Business Zone system.

- **Confirmation of transaction**
  In the context of business social responsibility, those involved in trading digital assets are expected to implement measures to prevent the transfer of criminal proceeds, as is the case with other models. Depending on the risk level and necessity, the following information is obtained from the end user and recorded: the nature of the digital assets handled, the purpose of the digital asset trading, and the destination of the digital assets transferred. Suspicious transactions are detected based on this information. While Business Zone service providers do not have direct control over the transfer of digital assets, it is recommended that they monitor the distributed ledger that manages the end user's digital assets and monitor digital assets that have been transferred since the transaction was made through the Business Zone system for a certain period.

4.7 Responding to Security Issues for Model 3

- **End-user identity proofing and authentication**

  As in Model 1, Business Zone service providers are responsible for safeguarding digital assets and ensuring adequate identification of end users. This protects consumers and prevents the transfer of criminal proceeds. In accordance with legal and regulatory requirements as well as industry standards, the nature of digital assets dictates that Business Zone service providers must implement appropriate identity proofing process and authentication methods with sufficient stringency, depending on the level of overall risk for the business.

- **System-wide security measures for the Business Zone**

  As in Model 1, the Business Zone system must be managed securely in line with the characteristics of the distributed ledger system being connected. The fundamental premise is that in a private-permissioned distributed ledger, each node is required to operate in accordance with specific security standards to facilitate the effective implementation of the mechanism. It is essential to implement appropriate data backup procedures for nodes, along with security measures for the operating environment. It is the responsibility of the general nodes that view the ledger or transmit transactions to prevent unauthorized access to the distributed ledger system. The number of nodes with transaction authorization and ledger generation roles (privileged nodes) is more limited than that in a public permissionless distributed ledger. Consequently, these nodes bear a greater responsibility for maintaining the security of the entire distributed ledger system.

  To ensure the security of individual private nodes and the overall integrity of the distributed ledger system, it is essential that each distributed ledger system establishes security standards for both general and privileged nodes. These standards must be strictly adhered to by all nodes within the system. Furthermore, a third-party assessment of compliance with the standards is conducted, as necessary. The results of this assessment may inform decisions on whether to connect to a relevant distributed ledger system. Maintaining a consistent security standard for each node connected to a private permissionless distributed ledger system would also facilitate collaboration between the administrators of each node to efficiently address issues that may arise in the distributed ledger system. It is also important to consider the physical arrangement of the nodes to achieve fault tolerance and security through node distribution.

- **Confirmation of transaction**

  As in Model 1, transactions should be confirmed and monitored according to risk and necessity.

05

Conclusion

Solving or Mitigating Security Issues

The security of distributed ledgers, which can be the basis for digital asset transactions and the utilization and coordination of important data, is of great importance. It is crucial for both the operators and users of distributed ledgers to understand their nature and handle them appropriately. As previously discussed, distributed ledger technology is a complex field encompassing various technological elements, including cryptography and distributed processing technology. Any vulnerability in these elements can have a significant impact, and in severe cases, can lead to the malfunctioning of the entire distributed ledger system.

The security of a distributed ledger depends on the security of the individual technical elements, the security of the combination of these elements, and the security provided by the distributed ledger system, which is composed of a network of many nodes. In particular, public permissionless distributed ledgers are often more challenging to evaluate because of the economic mechanisms involved in maintaining security through cryptographic assets and token issuance. Furthermore, it is essential to assess the security of the surrounding environment, including the smart contract framework and wallets that manage the signature keys.

This document provides a comprehensive overview of the technical aspects of distributed ledger security, outlining key considerations and mitigation strategies for designing and operating a system in a Business Zone that utilizes distributed ledgers. These considerations include assessing the likelihood of threats and potential impact of any resulting damage. However, in addition to the difficulty of evaluation and rapid technological progress, it is challenging for individual operators to evaluate various distributed ledger platforms and distributed ledger systems. To encourage the adoption of more secure distributed ledger systems, the Digital Currency Forum and other industry organizations involved in distributed ledgers, the developer community, the user community, academia, security experts, and standardization bodies should work together to share case studies on security measures and actual risk responses related to distributed legers, to gain a deeper understanding, establish guidelines, evaluate implementations, and create a list of recommended implementations.

References

1. ISO 23257:2022 Blockchain and distributed ledger technologies
   Reference architecture
   https://www.iso.org/standard/75093.html

2. X.1401 : Security threats of distributed ledger technology
   https://www.itu.int/rec/T-REC-X.1401-201911-I/en

3. X.1402 : Security framework for distributed ledger technology
   https://www.itu.int/rec/T-REC-X.1402-202007-I/en

Security Review Report

Analysis of Threats and Mitigation Measures Based on Blockchain Connection Patterns

Editor & Author	Lead Company of the Wallet Security Subcommittee (SECOM CO.,LTD.) **Masashi Sato** (Intelligent Systems Laboratory, SECOM CO.,LTD.) **Haruki Kondo** (Secom Trust Systems Co.,Ltd.) The Secretariat of the Wallet Security Subcommittee, The Secretariat of the Digital Currency Forum (DeCurret DCP Inc.)
Translation Contributor	**Satomi Tsujita** (En-sam-ble K.K.)
Issued by	The Secretariat of the Digital Currency Forum (DeCurret DCP Inc.)

The information in this Report, or on which this Report is based, has been obtained from sources believed to be reliable, but no guarantee or warranty is made regarding the accuracy or completeness of such information.We do not accept responsibility for any omissions, errors, or damages caused by the use of this information. Furthermore, even if future projections change due to circumstances arising after the creation of this document, the Digital Currency Forum, Wallet Security Subcommittee (hereafter, “this Subcommittee”) is not obliged to revise it. This document contains information about future projections ("projections"), and the subcommittee has made statements based on these projections. However, they represent the subcommittee's judgment at the present time, and the actual process and results may differ significantly. Therefore, please consider the associated uncertainties and risks. The Subcommittee cannot be held responsible for any damages incurred in relation to this document. This document contains confidential information that is the property of the members of this subcommittee. The copyright of this document belongs to the members of this subcommittee and is protected by copyright law and international treaties. Quoting, reproducing, adapting, or publicly transmitting any part or all of this document without prior written permission from this subcommittee, through the Digital Currency Forum Secretariat, is strictly prohibited.